JP3949679

Publication Title:

STEGANOGRAPHIC SYSTEM

Abstract:

Abstract of JP 2005051793

(A) PROBLEM TO BE SOLVED: To improve a steganographic system and applications therefor, more particularly to facilitate scale and rotation registration for steganographic decoding, to decode without accessing originals which are not coded, to increase robustness of steganographic coding and/or in the presence of lossy compression/decompression, and to make energy in a spatial domain facilitate decoding registration in motion pictures.

---

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-51793
(P2005-51793A)
(43)公開日　平成17年2月24日(2005.2.24)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04N 1/387	H04N	1/387		5B057
G06T 1/00	G06T	1/00	500B	5C076

審査請求 有　請求項の数 46　ＯＬ　（全 115 頁）

(21)出願番号	特願2004-224727(P2004-224727)
(22)出願日	平成16年7月30日(2004.7.30)
(62)分割の表示	特願平8-534258の分割
原出願日	平成8年5月7日(1996.5.7)
(31)優先権主張番号	08/436,102
(32)優先日	平成7年5月8日(1995.5.8)
(33)優先権主張国	米国(US)
(31)優先権主張番号	08/508,083
(32)優先日	平成7年7月27日(1995.7.27)
(33)優先権主張国	米国(US)
(31)優先権主張番号	08/512,993
(32)優先日	平成7年8月9日(1995.8.9)
(33)優先権主張国	米国(US)
(31)優先権主張番号	08/534,005
(32)優先日	平成7年9月25日(1995.9.25)
(33)優先権主張国	米国(US)

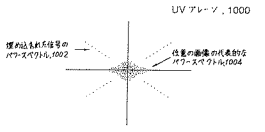
(71)出願人　500111792
ディジマーク　コーポレイション
アメリカ合衆国　オレゴン州　９７００８，ビーヴァートン，　エスダブリュー　ジェミニ　ドライヴ　９４０５
(74)代理人　100094318
弁理士　山田　行一
(72)発明者　ローズ　ジェフリー　ビー
アメリカ合衆国　オレゴン州　９７０６８　ウェスト　リン　エスダブリュー　トゥアラテン　ループ　３０４

Ｆターム(参考)　5B057 AA20 CA12 CA16 CB12 CB16 CB19 CE08 CH20 DA20 DB02
5C076 AA14 BA06

最終頁に続く

(54)【発明の名称】ステガノグラフィシステム

(57)【要約】　（修正有）
【課題】ステガノグラフィシステムおよびその用途の改善であり、具体的にはステガノグラフィ的復号化に関するスケールおよび回転整合を容易にすること、符号化されていないオリジナルにアクセスすることなく復号化すること、動画におけるおよび／または損失的圧縮／伸張のステガノグラフィ的符号化の堅牢性を増すことと、空間領域におけるエネルギが復号化整合を容易にすることである。
【解決手段】回転対称にステガノグラフィ的に埋め込まれたパターン、およびサブリミナルディジタルグラティキュールを使用し、パターン化ビットセルによってデータを表す。用途は、拡張セキュリティ金融商取引と、偽造防止識別カードと、セルラ電話用詐欺抑止システムと、ビデオ送信における隠れモデムチャネルと、自動著作権検出を有する写真複写キオスクと、インターネットにおいて使用する、例えば、ＵＲＬを埋め込まれたホットリンク化画像オブジェクトとを含む。
【選択図】図２９



空間領域におけるクロスハッチングパターンのような波を生じる、45度軸に沿った非調和空間周波数

【特許請求の範囲】
【請求項1】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法は、
　　画像画素を含むディジタル画像を受信する工程と、
　　前記ディジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、
　　識別コードを表す２次元のコード信号を生成する工程であって、前記２次元コード信号は、ディジタル画像での位置に対応している要素を有し、且つ前記位置上で識別コードがランダム化されて繰り返し分布されるよう生成される、前記生成工程と、
　　２次元コード信号に基づいてディジタル画像を変更することによって、識別コードをディジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、
を含む方法。
【請求項2】
前記識別コードはURLアドレスを備える、請求項１に記載の方法。
【請求項3】
前記識別コードは、ネットワーク資源を見つけるのに用いられるインデックスを備える、請求項１に記載の方法。
【請求項4】
前記識別コードは、前記２次元コード信号のブロックで繰り返される、請求項１に記載の方法。
【請求項5】
前記オブジェクトに登録データをステガノグラフィ的に埋め込み、前記オブジェクトの印刷バージョンから画像を走査することによって生じる回転およびスケール変更を補正する、請求項１に記載の方法。
【請求項6】
前記登録データは、周波数領域でパターンを備える、請求項５に記載の方法。
【請求項7】
前記登録データは、前記２次元コード信号によって形成されるパターンを備える、請求項５に記載の方法。
【請求項8】
前記２次元コード信号は、ディジタル画像の対応する画素に応じて変化して、前記オブジェクトでの識別コードの知覚可能性を低減する、請求項１に記載の方法。
【請求項9】
前記２次元コード信号は、前記ディジタル画像から独立している鍵に従属している、請求項１に記載の方法。
【請求項10】
前記鍵は、データオブジェクトで識別コードをランダム化するのに用いられる、請求項１に記載の方法。
【請求項11】
前記識別コードは、オブジェクトをネットワーク上のデータベースに関連づけているインデックス情報を含む、請求項１に記載の方法。
【請求項12】
前記ディジタル画像はカラー画像を備え、前記ステガノグラフィック埋め込みは前記カラー画像の輝度を変更することによって実行される、請求項１に記載の方法。
【請求項13】

前記識別コードは２以上のビットを含み、前記２次元コード信号は、前記オブジェクトの複数の画素のそれぞれが２ビット以上の情報によって変更されるように、前記ディジタル画像を変更する、請求項１に記載の方法。
【請求項14】
前記２次元コード信号の要素は前記ディジタル画像の画素ブロックに対応し、前記要素は、前記画素ブロックの特徴を変調して前記識別コードを埋め込む、請求項１に記載の方法。
【請求項15】
前記要素は、低周波数に前記識別コードの信号エネルギが集中するように前記画素ブロックの特徴を変調する、請求項１４に記載の方法。
【請求項16】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、
　　前記オブジェクトの画像を走査して、前記オブジェクトを表す画像画素を含むディジタル画像を形成する工程と、
　　前記ディジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記ディジタル画像にステガノグラフィ的に埋め込まれた２次元のコード信号で運ばれ、前記２次元コード信号は、ディジタル画像内の位置に対応している要素を有し、前記２次元コード信号は、前記位置上で前記識別コードをランダム化して、繰り返し分布している、前記工程と、
　　前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトから前記ネットワーク資源へのナビゲーションを可能にしている、前記工程と、
を含む方法。
【請求項17】
前記ディジタル画像の特徴を解析して前記識別コードのビットを抽出する工程を含む、請求項１６に記載の方法。
【請求項18】
前記ディジタル画像の統計的特徴を解析して前記識別コードのビットを抽出する工程を含む、請求項１７に記載の方法。
【請求項19】
前記ディジタル画像の画素ブロックの特徴を解析して前記識別コードのビットを抽出する工程を含む、請求項１７に記載の方法。
【請求項20】
異なる極性が前記識別コードのビットの異なるビット値を伝達するのに用いられる、請求項１６に記載の方法。
【請求項21】
前記ディジタル画像の画素のそれぞれが前記識別コードの２以上のビットを伝達する、請求項１６に記載の方法。
【請求項22】
前記識別コードはURLアドレスを備える、請求項１６に記載の方法。
【請求項23】
前記識別コードは、ネットワーク資源を見つけるのに用いられるインデックスを備える、請求項１６に記載の方法。
【請求項24】
前記識別コードは、前記２次元コード信号のブロックで繰り返される、請求項１６に記載の方法。
【請求項25】
前記ディジタル画像から登録データをステガノグラフィ的に復号化し、前記オブジェクト

の印刷バージョンから画像を走査することによって生じる回転およびスケール変更を補正する、請求項１６に記載の方法。
【請求項26】
前記登録データは、周波数領域でパターンを備える、請求項２５に記載の方法。
【請求項27】
前記登録データは、前記２次元コード信号によって形成されるパターンを備える、請求項２５に記載の方法。
【請求項28】
前記２次元コード信号は、前記ディジタル画像から独立している鍵に従属している、請求項１６に記載の方法。
【請求項29】
前記鍵は、前記ディジタル画像から前記識別コードのビットを復号するのに用いられる、請求項２８に記載の方法。
【請求項30】
前記鍵がランダム特性を有する、請求項２９に記載の方法。
【請求項31】
前記識別コードは、オブジェクトをネットワーク上のデータベースに関連づけているインデックス情報を含む、請求項１６に記載の方法。
【請求項32】
前記ディジタル画像はカラー画像を備え、前記ステガノグラフィ的復号化は前記カラー画像の輝度から前記識別コードのビットを抽出することによって実行される、請求項１６に記載の方法。
【請求項33】
幾何登録は、前記画像をステガノグラフィ的に埋め込まれた登録パターンに相関させることによって実行される、請求項１６に記載の方法。
【請求項34】
相関を実行して、前記ディジタル画像から前記識別コードのビットを抽出する工程を含む、請求項１６に記載の方法。
【請求項35】
エラー訂正コーディングを用いて、前記ディジタル画像から前記識別コードのビットを抽出する工程を含む、請求項１６に記載の方法。
【請求項36】
信頼性の重み付けを用いて、前記識別コードのビット値を抽出する際にエラーを低減する工程を含む、請求項３５に記載の方法。
【請求項37】
オブジェクトから、ネットワークに記憶された前記オブジェクト関連の情報へのナビゲーションを管理するシステムであって、前記システムは、
　　オブジェクトにステガノグラフィ的に埋め込まれた識別コードの登録所であって、前記識別コードおよび前記ステガノグラフィックコードが埋め込まれた前記オブジェクト関連情報を記憶している、前記登録所と、
　　前記オブジェクトからステガノグラフィ的に復号化される識別コードを受信するサーバであって、前記識別コードを用いて前記オブジェクト関連情報を得るのに使用可能な、前記サーバと、
を備えるシステム。
【請求項38】
前記サーバおよび登録所は、インターネットからアクセスでき、前記オブジェクトから復号化された前記識別コードに応じてオブジェクト関連情報を提供する、請求項３７に記載のシステム。
【請求項39】
前記識別コードはURLアドレスを備える、請求項３７に記載のシステム。

【請求項40】
前記識別コードがデータベースへのインデックスを備え、前記データベースは、前記インデックスに対応するアドレス情報を記憶し、前記アドレス情報は、前記オブジェクトに関連したネットワーク資源をナビゲートするのに用いられる、請求項３７に記載のシステム。
【請求項41】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法を実行する命令を格納する記憶媒体であって、
前記方法が、
　　画像画素を含むディジタル画像を受信する工程と、
　　前記ディジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、
　　前記識別コードを表す２次元のコード信号を生成する工程であって、前記２次元コード信号はディジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードがランダム化されて繰り返し分布されるよう生成される、前記生成工程と、
　　２次元コード信号に基づいてディジタル画像を変更することによって、識別コードをディジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、
を含む、記憶媒体。
【請求項42】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法を実行する命令を格納する記憶媒体であって、
前記方法が、
　　前記オブジェクトの画像を走査して、前記オブジェクトを表す画像画素を含むディジタル画像を形成する工程と、
　　前記ディジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記ディジタル画像にステガノグラフィ的に埋め込まれた２次元のコード信号で運ばれ、前記２次元コード信号は、ディジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードをランダム化して、繰り返し分布している、前記工程と、
　　前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、
を含む、記憶媒体。
【請求項43】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法は、
　　画像画素を含むディジタル画像を受信する工程と、
　　前記ディジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、
　　識別コードを表す２次元のコード信号を生成する工程であって、前記２次元コード信号はディジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードが繰り返し分布されるよう生成される、前記生成工程と、
　　２次元コード信号に基づいてディジタル画像を変更することによって、識別コードをディジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーション

を可能にする、前記生成工程と、
を含む方法。
【請求項44】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法は、
画像画素を含むディジタル画像を受信する工程と、
前記ディジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、
識別コードを表す２次元のコード信号を生成する工程であって、前記２次元コード信号はディジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードがランダム化されて分布されるよう生成される、前記生成工程と、
２次元コード信号に基づいてディジタル画像を変更することによって、識別コードをディジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、
を含む方法。
【請求項45】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、
前記オブジェクトの画像を走査して、前記オブジェクトを表す画像画素を備えているディジタル画像を形成する工程と、
前記ディジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記ディジタル画像にステガノグラフィ的に埋め込まれた２次元のコード信号で運ばれ、前記２次元コード信号は、ディジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードをランダム化している、前記工程と、
前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、
を含む方法。
【請求項46】
オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、
前記オブジェクトの画像を走査して、前記オブジェクトを表す画像画素を備えているディジタル画像を形成する工程と、
前記ディジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記ディジタル画像にステガノグラフィ的に埋め込まれた２次元のコード信号で運ばれ、前記２次元コード信号は、ディジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードを繰り返し分布している、前記工程と、
前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、
を含む方法。

【発明の詳細な説明】
【ステガノグラフィの背景】
【0001】
ステガノグラフィに対する多数のアプローチと、ステガノグラフィの多数の用途とが存

在する。概略は以下の通りである。

【0002】

ソーン　イー　エム　アイに対する英国特許公開明細書第２１９６１６７号は、オーディオ記録を記録のオーナを示すマーキング信号と電子的に混合し、その組み合わせがオリジナルと知覚的に同一であるシステムを開示している。米国特許明細書第４９６３９９８号および第５０７９６４８号は、このシステムの変形例を開示している。

【0003】

ボルト、ベレナックおよびニューマンに対する米国特許明細書第５３１９７３５号は、前述のソーン　イー　エム　アイの特許と同じ原理に基礎を置いているが、精神音響マスキング問題を追加で述べている。

【0004】

モーゼスに対する米国特許明細書第４４２５６４２号、第４４２５６６１号、第５４０４３７７号および第５４７３６３１号は、データをオーディオ信号にごくわずかに埋め込む種々のシステムを開示しており、後者の２つの特許は、特に、ニューラルネットワーク実現化と、細部の知覚的符号化とに焦点をおいている。

【0005】

エー　ティー　アンド　ティーに対する米国特許明細書第４９４３９７３号は、低レベルノイズ信号を他のデータに追加し、これらと共に補助データを伝送する拡張スペクトル技術を用いるシステムを開示している。この特許は、ネットワーク制御信号をディジタル化音声信号と共に送信する状況において特に説明している。

【0006】

ユー　エス　フィリップスに対する米国特許明細書第５１６１２１０号は、追加の低レベル量子化レベルを、オーディオ信号において規定し、これらと共に、例えば、コピー禁止信号を伝送するシステムを開示している。

【0007】

グロスに対する米国特許明細書第４９７２４７１号は、著作権が取得された素材に関するオーディオ（例えば、ラジオ）信号の、これらに識閾下的に埋め込まれた識別信号の参照による自動的な監視において援助することを目的とするシステムを開示している。

【0008】

デジーンに対する米国特許明細書第５２４３４２３は、ランダムに選択されたビデオラインにおいてディジタルデータ（例えば、番組企業識別、著作権マーキング、媒体調査、非公開説明、等のデータ）を符号化するビデオステガノグラフィシステムを開示している。デジーンは、テレビジョン同期パルスに頼り、ディジタルデータによってＸＯＲされ、ビデオと結合された格納された疑似ランダムシーケンスをトリガする。

【0009】

欧州特許出願公開明細書第５８１３１７号は、画像を多ビット識別コードと共に冗長的にマーキングするシステムを開示している。前記コードの各々の“１”（“０”）ビットを、複数の間隔を置いて離れた“署名点”の周囲の画素値におけるわずかな増加（減少）として明らかにする。疑わしい画像とオリジナルの非符号化画像との差を計算し、前記署名点の周囲の画素変動を検査することによって復号化を進める。

【0010】

ＰＣＴ明細書ＷＯ９５／１４２８９号は、この分野における本願明細書に先行する仕事である。

【0011】

コマツ他は、彼らの論文“文書画像通信における電子透かしにおける提案と、署名を実現化するためのその用途”、日本における電子および通信、パート１、７３巻、Ｎｏ．５、１９９０年、２２～３３ページにおいて、画像マーキング技術を説明している。この仕事は、理解することがいくらか困難であるが、透かし（例えば、１ビット符号化メッセージ）が疑わしい画像において存在するかどうかの単純なイエス／ノー決定に明らかに帰着する。

【0012】
ビデオ信号へのディジタル情報の埋め込みに関する多数の仕事が存在する。多くは、垂直および水平帰線消去期間のような信号の非視覚的部分への埋め込みを行うが、他のものは、この情報を“バンド内”（すなわち、可視ビデオ信号それ自身）に埋め込む。例は、米国特許明細書第４５２８５８８号、第４５９５９５０号および第５３１９４５３号と、欧州特許出願公開明細書第４４１７０２号と、マツイ他、“ビデオステガノグラフィ：署名を画像に秘密に埋め込む方法”、アイ　エム　エー知的財産プロジェクト会報、１９９４年１月、１巻、第１版、１８７～２０５ページとを含む。

【0013】
ビデオおよびマルチメディアの著作権マーキングにおいて、ヨーロッパにおいて種々のコンソーシアムの研究の試みが存在する。技術の概説は、“画像のアクセス制御および著作権保護（ＡＣＣＯＰＩ）、ワークパッケージ８：透かし”１９９５年６月３０日、４６ページにおいて見られる。タリスマンと呼ばれる新たな計画は、このＡＣＣＯＰＩ仕事をある程度拡張すると思われる。これらの計画において活動的な研究者ザオおよびコーは、シスコップとして知られるウェブを基礎とする電子媒体マーキングサービスを提供している。

【0014】
オーラは、彼の論文“不可視通信”、ヘルシンキ技術大学、ディジタルシステム研究室、１９９５年１１月５日において、ステガノグラフィの多数の問題を調査している。

【0015】
スタンフォード２世他は、“データ埋め込み方法”、ＳＰＩＥ　２６１５巻、１９９５年１０月２３日において、彼らの１９９４年５月の動作である、画像ステガノグラフィプログラム（ＢＭＰＥＭＢＥＤ）を報告している。

【0016】
英国の企業、ハイウォータ　エフビーアイリミテッドは、識別情報を写真および他のグラフィカルデータにごくわずかに埋め込むソフトウェア製品を紹介している。この技術は、欧州特許明細書第９４００９７１．９（１９９４年１月１９日出願）、第９５０４２２１．２号（１９９５年３月２日出願）および第９５１３７９０．７号（１９９５年７月３日出願）とに属し、これらの最初のものは、ＰＣＴ国際公開パンフレットＷＯ９５／２０２９１号として公開されている。

【0017】
エムアイティのウォルター　ベンダーは、彼の論文、“データハイディングに関する技術”、マサチューセッツ工科大学、メディア研究室、１９９５年１月にによる説明のように、この分野における種々の仕事を行っている。

【0018】
パロアルトのダイス社は、アージェントの名の下で示されるオーディオマーキング技術を開発している。米国特許が未決定であることが理解され、まだ発行されていない。

【0019】
ティルケル他は、モナッシュ大学において、例えば、“電子すかしマーク”，DICTA-93，マッカリー大学，シドニー，オーストラリア，　１９９３年１２月と、“電子すかし”ＩＥＥＥ　画像における国際会議，１９９４年１１月１３－１６日，８６－９０ページとを含む種々の論文を発表している。

【0020】
ＮＥＣテクニカルリサーチインスティテュートのコックス他は、“マルチメディアの保障拡張スペクトルすかし”と表題の付いた１９９５年１２月の彼らの論文において、種々のデータ埋め込み技術を考察している。

【0021】
モレー他は、“Rechnergetutzte Steganographic: Wie sie Funktioniert undwarum folglish jede Reglementierung von Verschlusselung unsinnig ist,”DuD Datenschtz und Datensicherung, 18/6(1994) 318-326 において、ＩＳＤＮにおいて補助データを命令

的に埋め込む実験的なシステムを考察している。このシステムは、ＩＳＤＮ信号標本を取り上げ、変更し、しきい値以下の標本信号に関する補助データ送信を引き上げる。

【0022】

一般的に、隠すべきメッセージストリームからのビットを画像またはオーディオ信号の最下位ビットと交換することによって動作する、インターネット（例えば、“ステゴ”および“ホワイトノイズストーム”において利用可能な種々のソフトウェアプログラムが存在する。

【0023】

詳細な説明

説明的な実施例の以下の論考において、言葉“信号”および“画像”を、１、２および２を越える偶数の次元のディジタル信号に言及するのに交換可能に使用する。例を、１次元オーディオ形式ディジタル信号と２次元画像形式ディジタル信号との間で前後に慣例的に切り換える。

【0024】

本発明の説明的な実施例の詳細を十分に説明するために、最初にディジタル信号の基本的な性質を説明することが必要である。図１は、１次元ディジタル信号の古典的な表現を示す。ｘ軸は、ディジタルの配列“標本”のインデックス番号を規定し、ｙ軸は、ディジタル標本の“２進深度”として規定される有限数のレベルのみにおける存在に抑制されている標本における信号の瞬間的な値である。図１に示す例は、標本値の１６の許可された状態を与える４乗または“４ビット”に対して２の値を有する。

【0025】

音波のようなオーディオ情報に関して、ディジタル化処理は、連続した現象を時間領域および信号レベル領域の双方において離散的に取り扱うと、一般的に認識されている。そのようなものとして、ディジタル化の処理それ自身が、基本的なエラー原因をもたらし、いずれかの領域における離散的な処理期間より小さい細部を記録することができない。産業界はこれを、時間領域において“エイリアシング”と呼び、信号レベル領域において“量子化ノイズ”と呼ぶ。このように、ディジタル信号の基本エラーフロアが、常に存在する。実効的意味において測定された純粋な量子化ノイズは、１２の平方根を１越えた値か、０．２９ＤＮ程度の値を有することが理論的に既知であり、ここでＤＮは、“ディジタル数”または信号レベルの最も細かい単位増分を表す。例えば、完全な１２ビットディジタイザは、～０．２９ＤＮの固有実効ノイズフロアを伴う、４０９６の許可されたＤＮを有する。

【0026】

すべての既知の物理測定処理は、連続信号のディジタル形式への変換に追加のノイズを加える。代表的に量子化ノイズは、後に言及するように、直角位相（二乗平均の平方根）において、測定処理の“アナログノイズ”に加わる。

【0027】

ほとんどすべての商業的および技術的処理によるデシベルスケールの使用は、所定の記録媒体における信号およびノイズの測定として使用される。“信号－ノイズ比”という表現は、一般に、本明細書におけるように使用される。例として、本明細書は、信号ノイズ比を、信号パワーおよびノイズパワーの項として言及し、したがって２０ｄＢは、信号振幅における１０倍の増加を表す。

【0028】

要約において、本発明の現在の好適な実施例は、全体の信号に、純粋なノイズの形状を有する非常に小さい振幅の符号化信号の付加によってＮビット値を埋め込んだ。通常Ｎを、少なくとも８とし、Ｎビット値の復旧および復号化における最終的な信号－ノイズの考慮によって、より高い限度にする。実際的な問題として、Ｎを、所望の固有の異なった“署名”の数のような、用途の特定の理由に基づいて選択する。説明するために、Ｎ＝１２８とすると、固有のディジタル署名の数は、１０＾＾３８（２＾＾１２８）以上になる。この数は、十分な統計的な確実性をもって作品を検証することと、情報の正確な販売およ

び配布を示すことの双方に対して十分な値以上であると思われる。

【0029】

この追加の信号の振幅またはパワーは、この方法論を使用する各々すべての用途の、審美的なおよび情報の考慮によって決定する。例えば、非職業的なビデオは、平均的な人間の眼に目立つことなしに、より高い埋め込み信号レベルを有することができるが、高精度オーディオは、“ヒス”における不快な増加を人間の耳が知覚しないように比較的小さい信号レベルのみを採用することができる。これらの供述は、一般的なものであり、各々の用途は、埋め込み信号の信号レベルの選択において、それ自身の基準の組を有する。埋め込み信号のより高いレベルは、より悪質なコピーを検証することができる。他方では、埋め込み信号のより高いレベルは、より不快な知覚されるノイズが、もしかすると配布される作品の価値に影響を及ぼすかもしれない。

【0030】

本発明の原理を用いることができる異なった用途の範囲を説明するために、本明細書は、２つの異なったシステムを詳述する。第１のもの（よりよい名前が無いために、“バッチ符号化”システムと呼ぶ）は、存在するデータ信号に検証符号化を用いる。第２のもの（よりよい名前が無いために、“リアルタイム符号化”と呼ぶ）は、発生された信号に検証符号化を用いる。これらの当業者は、本発明の原理を、特に記述したこれらに加えて、多くの他の状況に用いることができることを認識するであろう。

【0031】

これらの２つのシステムの論考を、どちらの順番で読むこともできる。何人かの読み手は、後者が前者より直観的であることに気づき、他の者にとっては、その反対が真実であろう。

【0032】

バッチ符号化

実施例の第１の組の以下の論考は、関連する用語を規定する段落によって最も良く始められる。

【0033】

オリジナル信号を、オリジナルディジタル信号か、非ディジタル信号の高品質にディジタル化されたコピーに適用する。

【0034】

Ｎビット検証ワードを、８から１２８までのＮレンジを代表的に有し、開示された変換処理を経て最終的にオリジナル信号において配置される検証コードである、固有検証２進値に適用する。示された実施例において、各々のＮビット検証ワードは、値“０１０１”の配列から始まり、疑わしい信号（後述する定義を参照）における信号－ノイズ比の最適化を決定するのに使用される。

【0035】

Ｎビット検証ワードのｍ番目のビット値を、Ｎビットワードの左から右に読んだときのｍ番目の位置に値に対応するゼロまたは１のいずれかとする。例えば、Ｎ＝８検証ワード０１１１０１００の第１（ｍ＝１）ビット値は、値“０”であり、この検証ワードの第２ビット値は、“１”である、等。

【0036】

ｍ番目の独立埋め込みコード信号を、オリジナル信号に正確に等しい次元および量（例えば、双方が５１２かける５１２ディジタル画像）を有し、（示した実施例においては）ディジタル値の独立した擬似ランダムな配列である信号に適用する。“擬似”は、純粋なランダム状態を哲学的に決定する困難に敬意を払い、“ランダム”信号を発生する種々の許容しうる方法が存在することを示す。いかなる所定のオリジナル信号にも、関係する正確にＮ個の独立した埋め込みコード信号が存在する。

【0037】

許容しうる知覚されるノイズレベルを、どの位の“余分なノイズ”、すなわち次に記述する複合埋め込みコード信号の振幅を、オリジナル信号に追加し、販売または別な方法の

配布に対して許容しうる信号を依然として有していられるかの用途固有の決定に適用する。本明細書は、許容しうる代表的な値としてノイズにおける１ｄＢの増加を使用するが、これは、全く任意である。

【0038】

複合埋め込みコード信号は、オリジナル信号と正確に等しい次元および量（例えば、双方が５１２かける５１２ディジタル画像）を有し、Ｎの独立埋め込みコード信号の追加で固有の減衰を含む信号に適用する。独立埋め込みコードを、任意のスケールにおいて発生するが、複合信号の振幅は、前もってセットされた許容しうる知覚られるノイズレベルを越えてはならず、したがってＮの追加独立コード信号の“減衰”を必要とする。

【0039】

配布可能信号を、オリジナル信号に複合埋め込みコード信号を加えたものから成る、オリジナル信号とほぼ同様のコピーに適用する。これは、外部の社会に配布され、オリジナル信号より僅かに高いが許容しうる“ノイズ特性”を有する信号である。

【0040】

疑わしい信号を、オリジナルおよび配布された信号の全体的な外観を有し、そのオリジナルに検証が一致する可能性を疑われている信号に適用する。疑わしい信号がＮビット検証ワードに一致する場合、解析すれば分かる。

【0041】

この第１実施例の詳細な方法論は、Ｎビットワードをｍビット値の各々にこれらの対応する結果として複合信号中に蓄積される独立埋め込みコード信号を乗算することによってオリジナル信号に埋め込むことから始まり、完全に合計された複合信号を次に許容しうる知覚されるノイズ振幅に減衰させ、結果として得られるオリジナル信号に加えられた複合信号が配布可能信号になる。

【0042】

次にオリジナル信号とＮビット検証ワードとすべてのＮの独立埋め込みコード信号とを、安全な場所に格納する。次に疑わしい信号を見つける。この信号は、多数のコピー、圧縮および伸長、異なった間隔のディジタル信号への再標本化、ディジタルからアナログへそこから戻ってディジタル媒体への変換、またはこれらの項目のなんらかの組み合わせを受けたかもしれない。この信号が、依然としてオリジナルと同様に見える場合、すなわちその本質的な性質が、これらの変換およびノイズの付加のすべてによってまったく破壊されない場合、埋め込み信号のノイズ特性に対する信号に応じて、検証処理を、統計上の確実さのある目的の程度に機能させるべきである。疑わしい信号の改ざんの程度と、オリジナルの許容しうる知覚されるノイズレベルとを、検証の要求される信頼性レベルの２つのキーパラメータとする。

【0043】

疑わしい信号における検証処理を、疑わしい信号をディジタルフォーマットおよびオリジナル信号の範囲に再標本化および整列することによって始める。したがって画像が２の因子によって減少している場合、同じ因子によってディジタル的に増大させる必要がある。さらに、音楽の一部が“削除”されているが依然としてオリジナルと同じ標本化率を有する場合、オリジナルのこの削除部分を記録する必要があり、これを代表的に、２つの信号の局所ディジタル相関（通常のディジタル操作）を行い、これの見つけた遅延値を使用して、オリジナルの部分に対する切断部分を記録することによって行う。

【0044】

疑わしい信号をオリジナルに対して標本化間隔を一致させ記録すると、疑わしい信号の信号レベルを実効的意味においてオリジナルの信号レベルに一致させるべきである。これを、オフセット、２つの信号間のエラーの二乗平均の最小値を前記増幅及びガンマのパラメータの関数として使用することによって最適化されている前記３つのパラメータを探索することによって行うことができる。この点において規格化され記録された、または便利のために単に規格化された疑わしい信号を呼び出すことができる。

【0045】

このとき新たに適合された対は、規格化された疑わしい信号から減算されたオリジナル信号を有し、差信号を提供する。次に差信号を、Ｎ個の独立埋め込みコード信号と記録されたピーク相関値の各々と相互に関係させる。第１の４ビットコード（“０１０１”）を、０値および１値の平均値と、ノイズ値がより上質の信号を望むなら２つの信号の更なる整合との双方におけるキャリブレータとして使用する（すなわち、０１０１の最適な分離は、２つの信号の最適な整合を示し、Ｎビット検証信号の蓋然的な存在が存在することも示す）。

【0046】

結果として得られるピーク相関値は、０１０１キャリブレーション配列によって見つけられた０および１の平均値に近接することにより０および１に変換することができる浮動小数点数のノイズの組を形成する。疑わしい信号が本当にオリジナルから得られたものである場合、上述した処理から結果として得られる検証数は、オリジナルのＮビット検証ワードと一致し、“ビットエラー”統計が予測されたものか既知でないものかを示す。信号－ノイズの考慮は、検証処理においてあの種類の“ビットエラー”が存在する場合、検証のＸ％の確率の状態を導くことを決定し、ここでＸは、９９．９％であることが望まれる。疑わしい信号が本当にオリジナルのコピーではない場合、０および１の本質的にランダムの配列が発生し、結果として生じる値の分離の明らかな不足が発生する。すなわち、結果として得られる値をヒストグラムにプロットすると、Ｎビット検証信号の存在は強い２レベル特性を示すが、コードの非存在または異なったオリジナルの異なったコードの存在は、ランダムな正規分布状の形式を示す。このヒストグラムの分離は、検証に対して十分であるが、正確なバイナリ配列を客観的に再生できる場合、検証のより強い証拠となる。

【0047】

特別な例

カクテルパーティにおける二人の国家首席の高価な絵を手に入れ、この絵が市場においてある妥当な報酬を得るに値するのが確実であるとする。我々は、この絵を売ることを望み、許可されないまたは支払われない方法で使用されないことを保証する。このことと以下のステップとを、図２において要約する。

【0048】

この絵を、陽画のカラープリントに変換すると仮定する。我々は始めにこれを、代表的な光度測定スペクトル応答曲線を有する通常の高品質白黒スキャナによって、ディジタル化された形式に走査する（カラー画像の３原色の各々において走査することによって、ノイズ比に対してより良い最終的な信号を得ることができるが、このニュアンスは、基本的な処理を記述することに対しては重要ではない）。

【0049】

ここで、走査された画像は、１２ビットグレイ値または４０９６の許可されたレベルによって規定される精度のグレイスケールを有する４０００×４０００画素のモノクロームディジタル画像になると仮定しよう。我々は、これを、これが前記定義における“オリジナル信号”と同一であることを表す“オリジナルディジタル画像”と呼ぶ。

【0050】

走査処理の間、我々は、ディジタル値“３０”に対応する絶対的な黒を任意に設定する。我々は、オリジナルディジタル画像において存在する基本２ディジタル数実効ノイズに加えて、所定の画素の輝度値の平方根の理論上のノイズ（産業界において“ショットノイズ”として知られている）が存在することを見積もる。式において、我々は、

$$<\mathrm{RMS\ Noise}_{n,m}>=\mathrm{sqrt}(4+(V_{n,m}-30)) \quad (1)$$

を有する。ここで、ｎおよびｍは、画像の行および列において０から３９９９まで変動する簡単な表示値である。Ｓｑｒｔは、平方根である。Ｖは、オリジナルディジタル画像における所定の表示画素のＤＮである。ＲＭＳｎｏｉｓｅの周囲の<>括弧は、これが期待される平均値であることを単に意味し、ここで各々すべての画素が、ランダムエラーを個別に有することは明らかである。したがって、ディジタル数または“輝度値”として１２００を有する画素値に対して、我々は、その期待される実効ノイズ値がｓｑｒｔ（１２０

４）＝３４．７０であることが分かり、この値は、１２００の平方根である３４．６４にまったく近い。

【0051】

我々はさらに、画素の固有の輝度値の平方根が、正確に眼が最小の不快なノイズとして知覚する値ではないことを理解しており、したがって我々は、式、

$$<\text{RMS Addable Noise}_{n,m}>=X*\text{sqrt}(4+(V_{n,m}-30)^{\wedge}Y) \quad (2)$$

を提案する。ここで、XおよびYを、我々が調節する経験的なパラメータとして加えており、“ａｄｄａｂｌｅ”ノイズは、上述した定義による我々の許容しうる知覚されるノイズレベルに属するものである。我々はここで、我々が選択することができるXおよびYの正確な値はどの位なのかを実験しようと思うが、我々は、我々が処理の次のステップを実行するのと同時に行う。

【0052】

我々の処理の次のステップは、我々のＮビット検証ワードのＮを選択することである。我々は、６５５３６の可能な値を有する１６ビット主検証値が、画像が我々のものであることを検証するのに十分に大きく、我々が、我々が追跡を望む画像の１２８のコピーのみを直接販売すると決定し、７ビットに、最初の７ビットの奇数／偶数の加算（すなわち、最初の７ビットにおけるビットのエラー照合）用の第８ビットを加える。ここで必要な全体のビットは、０１０１キャリブレーション配列用４ビットと、主検証用１６ビットと、バージョン用８ビットとであり、我々はここで、最初の２８ビットにおける他のエラー照合値として他の４ビットを投入し、Ｎとして３２ビットを与える。最後の４ビットは、その４ビットを選択するために、多くの業界標準エラー照合方法の１つを使用することができる。

【0053】

我々はここで、１６ビット主検証数をランダムに決定し、例として、１１０１　０００１　１００１　１１１０を得る。すなわち、販売されたオリジナルの我々の第１のバージョンは、バージョン識別子としてすべて０を有し、エラー照合ビットは一致しなくなる。我々はここで、我々がオリジナルディジタル画像に埋め込む我々の固有３２ビット検証ワードを有する。

【0054】

これを行うために、我々は、我々の３２ビット検証ワードの各々のビットに対して、３２の独立したランダムの４０００×４０００の符号化画像を発生する。これらのランダム画像を発生する方法を示す。これらを発生する極めて多くの方法が存在する。明らかに最も簡単な方法は、オリジナル写真における走査に使用される同じスキャナにおいて、入力としてこの時だけ黒い画像を置き、次にこれを３２回走査することによってゲインを上昇させることである。この技術の欠点は、大容量のメモリが必要なことと、“固定パターン”ノイズが、各々の独立“ノイズ画像”の一部となることだけである。しかし、固定パターンノイズを、通常の“ダークフレーム”減算技術によって除去することができる。我々は、通常ゲイン設定において２ＤＮ実効ノイズを見つけるよりもむしろ、絶対黒平均値をディジタル数“１００”において設定すると仮定し、ここで我々は、各々すべての画素の平均値について１０ＤＮの実効ノイズを見つける。

【0055】

我々は次に、中間空間周波数バンドパスフィルタ（空間相乗）を、各々すべての独立ランダム画像に用い、これらから極めて高い空間周波数と極めて低い空間周波数とを本質的に除去する。我々は、幾何学的な歪みや、スキャナにおける汚れや、整合誤りのような簡単な現実世界のエラー源の大部分は、より低い周波数において現れ、我々は、これらの形式の改ざんを回避するために、より高い空間周波数における我々の検証信号に集中したいため、極めて低い周波数を除去する。同様に我々は、所定の画像の多数の世代のコピーや圧縮－伸長変換は、より高い周波数をどんな方法でも破壊する傾向があり、これらの周波数が最も減衰する傾向がある場合、これらの周波数中に多すぎる検証情報が位置する点が存在しないようにするために、より高い周波数を除去する。したがって、我々の新たな抽

出された独立ノイズ画像は、中央空間周波数によって支配される。実際的な特徴において、我々は我々のスキャナにおいて１２ビット値を使用し、我々はＤＣ値を効果的に除去し、我々の新たな実効ノイズは１０ディジタル数より僅かに少ないことから、これを、結果として得られるランダム画像として－３２から０を通って３１まで変動する６ビット値に圧縮することが有効である。

【0056】

次に我々は、対応する３２ビット独立検証ワードのビット値において１を有するランダム画像のすべてを互いに加算し、１６ビット署名整数画像における結果を蓄積する。これは、複合埋め込み信号の非減衰および非比例バージョンである。

【0057】

次に我々は、式２のＸおよびＹパラメータを変化させることによって、複合埋め込み信号をオリジナルディジタル画像に加えることによって視覚的に実験する。式において、我々は、以下の式においてＸの最大化と適切なＹを見つけることとを繰り返し、

$$V_{dist;n,m} = V_{orig;n,m} + V_{comp;n,m} * X * \mathrm{sqrt}(4 + V_{orig;n,m} - Y) \qquad (3)$$

ここで、ｄｉｓｔを候補配布可能画像に適用し、すなわち我々は、我々に許容しうる画像を与えるＸおよびＹを見つけることを視覚的に繰り返し、ｏｒｇをオリジナル画像の画素値に適用し、ｃｏｍｐを複合画像の画素値に適用する。ｎおよびｍは、画像の行および列を依然として示し、この操作を４０００×４０００画素の全てにおいて行うことを示す。符号Ｖは、所定の画素および所定の画像のＤＮである。

【0058】

ここで任意の仮定として、我々は、我々の視覚的実験が、オリジナル画像を候補配布可能画像と比較した場合、Ｘ＝０．０２５およびＹ＝０．６の値が許容しうる値であることを発見したと仮定する。すなわち、“追加ノイズ”を有する配布可能画像は、美的センスにおいてオリジナルに許容しうるほど近い。我々の独立ランダム画像が１０ＤＮ程度のランダム実効ノイズ値を有し、１６程度のこれらの画像を互いに加算することが複合ノイズを４０ＤＮ程度に増加させることから、０．０２５のＸ増加値が、追加の実効ノイズを１ＤＮ程度またはオリジナルにおける我々の固有ノイズの振幅の半分に戻すことに注意されたい。これは大雑把に言って、暗い画素値のノイズにおける１ｄＢであり、０．６のＹ値によって変化したより明るい画素においてより高い値に対応するものである。

【0059】

このようにこれらのＸおよびＹの２つの値によって、我々はここで、我々のオリジナルの配布可能コピーの第１バージョンを構成する。他のバージョンは、単に新たな複合信号を形成し、必要だと考えるならＸを僅かに変更する。我々はここで、オリジナルディジタル画像を、各々のバージョン用３２ビット検証ワードと、３２の独立ランダム４ビット画像と共に固定し、我々のオリジナルの疑わしい著作権侵害の我々の最初のケースを待つ。記憶方法、これは、オリジナル画像用に１４メガバイト程度、ランダム検証埋め込み画像用に３２×０．５バイト×１６０００００＝～２５６メガバイト程度である。これは、１つの高価な画像に関して完全に許容しうる。多少の記憶装置の節約は、簡単な無損失圧縮によって得ることができる。

【0060】

我々の画像の疑わしい著作権侵害の発見

我々は、我々の画像を販売し、数カ月後、見たところは我々の画像から切り取られ剽窃され、他の様式化された背景場面に置かれたものを見つける。この新たな“疑わしい”画像は、所定の雑誌出版の１００００コピーにおいて印刷されているとする。我々はここで、我々のオリジナル画像の一部が許可されない方法で実際に使用されているかどうかを決定しようとする。図３は、詳細を要約する。

【0061】

第１のステップは、前記雑誌の発行物を入手し、前記画像をその上に有するページを切り取り、この時、慎重に、しかし慎重に成り過ぎずに、普通の鋏を使用して背景画像から２つの図を切り取ることである。もし可能なら、我々は、２つの図を別々に切り取るより

も、１つの接続された部分のみを切り取る。我々は、これを黒い背景上に張り付け、このことは、視覚的検査を行うのを簡単にする。

【0062】

我々はここで、我々の安全が保証された場所からオリジナルディジタル画像を３２ビット検証ワードおよび３２の独立埋め込み画像と共に得る。我々は、オリジナルディジタル画像を、標準画像操作ソフトウェアを使用する我々のコンピュータスクリーン上に配置し、我々は、疑わしい画像の我々のマスクされた領域と同じ境界線に沿っておおまかに切断し、同時に同じ様にこの画像をおおまかにマスクする。“おおまか”という言葉を、正確な切断が必要でないことから使用し、これは単に検証統計が合理的に終了されるのを助ける。

【0063】

次に我々は、マスクされた疑わしい画像を再スケーリングし、我々のマスクされたオリジナルディジタル画像の寸法に大まかに適合させる、すなわち我々は、疑わしい画像を拡大または縮小し、それをオリジナル画像の上に大まかに重ね合わせる。我々がこの大まかな整合を行った後、我々は次に、これらの２つの画像を、自動化されたスケーリングおよび整合プログラムに投入する。このプログラムは、ｘ位置、ｙ位置および空間スケールの３つのパラメータを捜索し、２つの画像間の二乗平均されたエラーが、なんらかの所定のスケール変数とｘおよびｙオフセットとで与えられるという形態の利点を有する。これは、全く標準的な画像処理方法論である。代表的に、これを、大体において滑らかな補完技術を使用して行い、サブ画素精度に行う。探索方法を、多くのものの１つとすることができ、シンプレックス方法を代表的な１つとする。

【0064】

最適なスケーリングをし、ｘ－ｙ位置変数を見つけたら、次に、前記２つの画像の黒レベルと輝度ゲインとガンマとの最適化における他の探索を行う。再び使用すべき利点の形態は、二乗平均エラーであり、再びシンプレックスまたは他の探索方法論を、これら３つの変数の最適化に使用することができる。これらの３つの変数を最適化した後、我々は、これらの修正を疑わしい画像に用い、それを、オリジナルディジタル画像およびそのマスクの画素間隔およびマスキングとに正確に整合させる。我々はここで、これを基準マスクと呼ぶことができる。

【0065】

次のステップは、新たに規格化された疑わしい画像から基準マスク領域内のみオリジナルディジタル画像を減算することである。この新たな画像を、差画像と呼ぶ。

【0066】

次に、３２の独立ランダム埋め込み画像すべてに渡って、マスクされた差画像とマスクされた独立埋め込み画像との間の局所相関を行う。“局所”を、上述した探索手順中、発見された２つの画像の名目上の整合点間のオフセットの＋／－１画素のオフセット領域によって相関させるのを開始することのみが必要であるという概念に適用する。相関のピークを、０，０オフセットの名目上の整合点に極めて近くすべきであり、我々は、３×３相関値を互いに加算し、我々の３２ビット検証ワードの３２の独立ビットの各々に対する１つの総括的な相関値を与えることができる。

【0067】

すべての３２ビット位置とこれらの対応するランダム画像のすべてにこれを行った後、我々は、３２値の準浮動小数点配列を有する。最初の４値は、０１０１の我々のキャリブレーション信号を表す。我々はここで、第１および第３浮動少数点値の平均を取り、この浮動小数点値を“０”と呼び、第２および第４値の平均を取り、この浮動少数点値を“１”と呼ぶ。我々は次に、残りのすべての２８ビット値に進み、単にこれらがより近い平均値に基づいて“０”または“１”のいずれかを割り当てる。簡単に言うと、疑わしい画像が実際に我々のオリジナルのコピーの場合、埋め込み３２ビット結果コードは、我々の記録のそれと一致すべきであり、それがコピーでない場合、我々は全体的なランダム状態を得るべきである。３）コピーであるが検証番号と一致しない第３の可能性と、４）コピー

ではないが適合する第４の可能性があり得る、３）の場合において、処理の信号ノイズ比が重圧を受ける、すなわち“疑わしい画像”が正確にオリジナルの極めて粗末なコピーである場合にあり得、４）の場合において、我々が３２ビット検証番号を使用していることから基本的に４０億に１つの可能性がある。我々が４）を本当に心配する場合、我々は、同じ雑誌の異なった刊行物においてこれらのテストを行う第２の独立した試験場を単に有することができる。最後に、これらの値が何を与えるのかを考慮したエラーチェックビットの照合は、処理全体において最終的な出来るかぎり過剰な検査である。ノイズ対する信号が問題に成りうる状況において、これらのエラーチェックビットを、多すぎる害なしに除去することができる。

【0068】

利益

第１の実施例の完全な説明を、詳細な例によって記述した今、処理ステップとこれらの利点との理論的解釈を指摘することが適切である。

【0069】

前述の処理の最終的な利益は、検証番号を得ることが、差画像を準備する手段および方法と完全に独立していることである。すなわち、切断、整合、スケーリング、等のような差画像の準備の方法は、検証番号が存在しない場合、検証番号を発見するオッズが増加せず、真の検証番号が存在する場合、検証処理の信号－ノイズ比のみが役に立つ。検証用画像を準備する方法は、互いに異なっているかもしれず、一致を形成する多数の独立した方法論の可能性を提供する。

【0070】

オリジナル信号または画像の部分集合において一致を得る能力は、今日の情報に富んだ世界におけるキーポイントである。画像および音声部分の双方の切断および張り付けは、より一般的になり、このような実施例をオリジナル作品が不正に使用されている場合、コピーを検出するのに使用させる。最後に、信号ノイズ比の一致は、コピー作品それ自身がノイズまたは顕著な歪みのいずれかによって顕著に変化している場合のみ困難となり、これらの双方がコピーの商業的価値に影響し、その結果、このシステムを妨げようとすることは、商業的価値における費用の莫大な減少においてのみ行うことができる。

【0071】

本発明の初期の概念は、１つのみの“スノー状”画像またはランダム信号をオリジナル画像に付加する場合、すなわちＮ＝１の場合であった。この信号を“複合化”することは、この信号の存在または不在における判断を行う（一般的に統計的な）アルゴリズムを使用する、その後の数学的解析を含む。このアプローチを上述した実施例として放棄した理由は、前記信号の存在または不在の検出の確実性において固有の灰色領域が存在することである。“０”から“１”の間で選択する方法を規定する簡単な予め規定されたアルゴリズムと組み合わされた多数のビット段階すなわちＮ＞１への前方への変化によって、本発明は、専門的な統計的解析から、コイン投げのようなランダム２値事象を推定する分野に、確実な問題を変化させた。これは、裁判所および市場の双方における本発明の直観的な許容に関係する有力な特徴として見られる。この全体の問題に対する発明者の考えを要約する類似は、次のようなものである。１つの検証番号の捜索は、コイン投げを１回のみコールし、このコールを行うことを秘密の専門家に期待することに等しいが、本発明の上述したＮ＞１の実施例は、コイン投げをＮ回連続して正確にコールする明白に直観的な原理に期待する。この状況は、非常に苛立たせるものであり、すなわち、画像および音声部分がより小さい範囲を得た場合、１つの信号の存在の“改ざん”の問題である。

【0072】

Ｎ＞１の場合がＮ＝１の実施例よりも好適な実施例である他の理由は、Ｎ＝１の場合において、疑わしい画像を準備し操作する方法が、正の検証を行う可能性を得ることである。したがって、専門家が検証の決定を行う方法は、この決定の必須の部分となる。この決定を行う多数の数学的および統計的アプローチの存在は、いくつかのテストが正の決定を行い、一方他のテストが負の決定を行うという可能性を残し、種々の検証アプローチの相

対的な利点についての他の秘密の議論をもたらす。本発明のＮ＞１の好適実施例は、既知の個人コード信号を不正に使用する前処理以外は信号の前処理なしで“コイン投げをＮ回連続してコールする”可能性を増加することができる方法を提供することによって、この他の灰色領域を回避する。

【0073】

本システムの最も完全な説明は、業界標準および多数の独立したグループが、埋め込み検証番号の適用およびその解読における彼ら自身の手段または“企業内ブランド”を設定するようになる場合、見えてくるだろう。多数の独立したグループ検証は、本方法の最終的な目的をさらに強化し、これによって業界標準としての魅力が増強される。

【0074】

複合埋め込みコード信号の生成における真の極性の使用

上述した論考は、その目的を実行するためにバイナリ技術の０および１の形式論を使用した。特に、Ｎビット検証ワードの０および１は、これらの対応する独立埋め込みコード信号に直接乗算され、複合埋め込みコード信号を形成する（ステップ８、図２）。このアプローチは、その概念の簡単さを確かに有するが、埋め込みコードの記憶と共に埋め込みコード信号の０による乗算は、一種の非能率さを含む。

【0075】

Ｎビット検証ワードの０および１の性質の形式論を保持するが、これらの対応する埋め込みコード信号を減算させるワードの０を有することが好適である。したがって、図２のステップ８において、Ｎビット検証ワードにおいて“１”に対応する独立埋め込みコード信号を“加算”するだけよりも、Ｎビット検証ワードにおいて“０”に対応する独立埋め込みコード信号の“減算”も行う。

【0076】

一見して、これは、最終的な複合信号により明白なノイズを付加しているように見える。しかし、０から１へのエネルギ幅分離は増加し、したがって図２のステップ１０において使用される“ゲイン”を、相対して低くすることができる。

【0077】

我々は、この改良を、真の極性の使用と呼ぶことができる。この改良の主な利点を、“情報の効率”として大きく要約することができる。

【0078】

独立埋め込みコード信号の“知覚の直交性”

上述した論考は、一般にランダムノイズ状信号を独立埋め込みコード信号として使用することを考察した。これは、発生する信号の恐らく最も簡単な形式である。しかしながら、独立埋め込み信号の組に用いることができる情報最適化の形式が存在し、本出願人は´知覚の直交性´という題目の下に記述する。この用語は、この直交性が、検証情報の信号エネルギを最大化すると同時に、ある知覚しうるしきい値より下に保持すべきであるという現在の追加の要求による、ベクトルの直交性の数学的な概念に大まかに基づいている。他の方法において、埋め込みコード信号は、必然的に現実にランダムであることを必要としない。

【0079】

感光乳剤ベースの写真の領域における第１実施例の使用および改良

上述した論考は、写真作品に適用できる技術を概説した。以下の節は、この領域の詳細をさらに説明し、これら自身を広範囲な用途に適合させるいくらかの改良を開示する。

【0080】

論考すべき第１の領域は、ネガフィルム、プリント紙、トランスペアレンシ等のような慣例的な写真作品上に通し番号を前記入または前露光することを含む。一般に、これは、先験的に固有な通し番号（および含有的に所有権およびトラッキング情報）を写真作品中に埋め込む方法である。通し番号それ自体は、余白に追いやられるか、プリントされた写真の背景上にスタンプされるのに対比して、通常の露光された画像の恒久的な部分であり、コピーと別の位置と別の方法とを必要とする。ここで呼ぶ´通し番号´は、一般にＮビ

ット検証ワードと同義語であり、ここでのみ我々は、より一般的な業界用語を使用している。

【0081】

図２のステップ１１において、本開示は、“オリジナル〔画像〕”をコード画像とともに記憶することを命じる。次に図３のステップ９において、疑わしい画像からオリジナル画像を減算し、これによって、可能な検証コードにノイズおよび改ざんが蓄積されたもののすべてを加えたものか残るように命令する。したがって、以前の開示は、複合埋め込み信号なしにオリジナルが存在するという暗黙の仮定をおこなった。

【0082】

ここで、プリント紙および他のコピー製品を販売する場合において、これは依然としてこの場合、すなわち“オリジナル”が埋め込みコード無しに実際に存在し、第１実施例の基本的な方法論を用いることができる。オリジナルフィルムは、“非符号化オリジナル”として完全に良好に役立つ。

【0083】

しかしながら、前露光されたフィルムを使用する場合において、複合埋め込み信号がオリジナルフィルム上に予め存在し、したがって予め埋め込まれた信号と分離し、“オリジナル”は、決して存在しない。しかしながら、この後者の場合は、上記で説明した原理をどのように最適に使用するかにおいての観察とともに、ビットをより厳密に調査する（前者の場合は前記で概説した方法に固執する）。

【0084】

予め番号付けられたネガフィルム、すなわち、各々すべてのフレームに極めて微かな固有複合埋め込み信号を前露光されたネガフィルムの場合の変更の最も明白な点は、以前示した図３のステップ９において現れる。他の相違が確かに存在するが、信号をフィルム上にどの様に何時埋め込むか、コード番号および通し番号をどの様に記憶するか、等のような現実に主として論理的なものである。明らかに、フィルムの前露光は、フィルムの生成および包装の一般的な大量生産工程に大きな変化をもたらす。

【0085】

図４は、フィルムを前露光する１つの可能性のあるこれ以後の機構の図式的な略図である。“これ以後”を、すべての共通製造工程をすでに行った後に処理を行うことに適用する。結局、経済的規模が、この前露光工程をフィルム製造の連鎖中に直接に配置することを要求する。図４に示すものは、フィルム書き込みシステムとして既知である。コンピュータ１０６は、図２のステップ８において生成される複合信号をその蛍光スクリーン上に表示する。次にフィルムの所定のフレームを、この蛍光スクリーンの像を映すことによって露光し、このときの露光レベルを一般的に極めて微かに、すなわち一般的にごく僅かにする。明らかに、市場が、これをどの位僅かにすべきかの市場自身の要求、すなわち弁護士が見積もる加えられた“性質”のレベルを設定するであろう。フィルムの各々のフレームを、逐次的に露光し、一般にＣＲＴ１０２において表示される複合画像を各々すべてのフレーム毎に変化させ、これによってフィルムの各々のフレームに異なった通し番号を与える。変換レンズ１０４は、フィルムフレームの焦点変化面とＣＲＴ表面とを強調する。

【0086】

前露光ネガフィルムの場合における前述の実施例の原理の適用に戻ると、図３のステップ９において、“オリジナル”をその埋め込みコードとともに減算すると、コードがオリジナルの整数部分であることから、明らかにコードも同様に“消去”する。運良く、救済策が存在し、検証を依然として行うことができる。しかしながら、この実施例を改良する技術者は、前露光ネガの場合における検証処理の信号ノイズ比を、非符号化オリジナルが存在する場合の信号ノイズ比に近づけることを要求される。

【0087】

この問題の簡単な定義は、この点における順番である。疑わしい写真（信号）を仮定した場合、コードがどこかに存在する場合、埋め込み検証コードを見つける。この問題は、上述したようなノイズおよび改ざんの状況内だけでなく、ここでは取り込まれた画像とコ

ードとの間の結合の状況内でも、疑わしい写真内の各々すべての独立埋め込みコード信号の振幅の発見の１つに減少する。“結合”を、ここでは取り込まれた画像が相関に“ランダムにバイアスする”という概念に適用する。

【0088】

このように、信号結合のこの追加の項目を心に止めておくと、検証処理は、各々すべての独立埋め込みコードの信号振幅を見積もる（図３のステップ１２では相関結果を得るのに対して）。我々の検証コードが疑わしい写真中に存在する場合、発見される振幅は、“１”を割り当てられている正振幅と“０”を割り当てられている負振幅を有する両振幅に分割されている。我々の固有検証コードは、それ自身を明らかにする。他方で、このような検証コードが存在しない場合、または何か他のコードである場合、振幅のランダムガウス状分布は、値のランダムな寄せ集めによって見つかる。

【0089】

独立埋め込みコードの振幅をどの様に発見するかについてのいくつかの更なる詳細を与えることが残っている。再び、運良く、この厳密な問題は、他の技術上の用途において処理されている。さらに、この問題と少しの食料とを数学者と統計学者とで混み合っているいる部屋に投げ込めば、ある適当な期間の後、半ダースの最適化された方法論が必ず出で来るであろう。それは、ある程度きれいに定義された問題である。

【0090】

ある特別な例としての解決法は、天文学上の撮像の分野から生じる。ここで、成熟した先行技術は、“熱ノイズフレーム”を物体の所定のＣＣＤ画像から減算する。しかしながらしばしば、熱フレームの減算においてどの位のスケーリング係数を使用するのかは明確に既知ではなく、正確なスケーリング係数の探索が行われる。これは、明確に本実施例のこのステップの仕事である。

【0091】

一般的な習慣は、単に一般的な探索アルゴリズムをスケーリング係数において行い、スケーリング係数を選択し、新たな画像を、

新たな画像＝獲得された画像－スケーリング係数×熱画像　　（４）

によって形成する。

【0092】

新たな画像に高速フーリエ変換ルーチンを用い、最終的に、新たな画像の積分高周波内容を最小化するスケール係数を見つける。この個々の量の最小化による一般的な形式の探索操作は、非常に一般的である。したがって発見されたスケール係数は、探索された“振幅”である。考察されているがまだ実現されていない改良は、獲得された画像のより高い導関数と埋め込みコードとの結合を、見積もり、計算されたスケール係数から除去することである。すなわち、上述した結合による特定のバイアス効果が存在し、最終的には理論上および経験的な実験の双方によって明らかにされ除去されるべきである。

【0093】

信号または画像の変化の検出における使用および改良

全体として信号または画像を検証することの基本的な必要性から離れて、信号または画像に対して起こりうる変化を検出する多少偏在する必要性も存在する。以下の節は、前記実施例を、特定の変更および改良によって、この領域における有力な道具としてどのように使用することができるかを記述する。

【0094】

最初に要約するために、我々は、前記で概説した基本的な方法を使用して正に検証された所定の信号または画像を有すると仮定する。すなわち、我々は、そのＮビット検証ワードと、その独立埋め込みコード信号と、その複合埋め込みコードとを知っている。次に我々は、我々の所定の信号または画像内の複合コードの振幅の空間マップを全く簡単に形成することができる。さらに我々は、規格化マップ、すなわちある大域的平均値の周囲を変化するマップを与えるために、この振幅マップを既知の複合コードの空間振幅によって分割することができる。このマップの簡単な調査によって、我々は、明白に変化して、規格

化振幅の値が代表的なノイズおよび改ざん（エラー）に単に基づくしきい値のある統計上の組より低下するどの様な領域も、視覚的に検出することができる。

【0095】

振幅マップの形成の実施の詳細は、種々の選択を有する。１つは、上述した信号振幅の決定に使用したのと同じ手順を行うことであり、ここでは我々は、我々が調査している領域付近に中心が位置する正規重み関数を信号／画像のすべての所定の領域に乗算する。

【0096】

万能コード対カスタムコード

本明細書は、ここまでは、各々すべてのソース信号が独立埋め込みコード信号の自分自身の組をどのように有するのかを概説した。これは、オリジナルに加えて相当な量の追加のコード情報の記憶を必要とし、多くの用途には、より経済的な形式が適切であろう。

【0097】

あるこのような節約のためのアプローチは、一組のソース作品に共通の独立埋め込みコード信号の所定の組を有することである。例えば、我々の１０００枚の画像がすべて、独立埋め込みコード信号の同じ基本的な組を利用することができる。このときこれらのコードに必要とされる記憶は、ソース作品に必要とされる記憶全体のほんの一部となる。

【0098】

さらに、いくつかの用途は、独立埋め込みコード信号の万能組、すなわち配布された作品のすべての場合に同一のままであるコードを利用することができる。この形式に必要なものは、Ｎビット検証ワードそれ自身を隠そうとし、このワードを読み取ることができる統一された装置を有するシステムによって分かるであろう。これを、読み取り位置の点において判断する／しないシステムにおいて使用することができる。この設定をする潜在的な欠点は、万能コードは、より追跡または盗難されやすく、したがってこれらは、前記で開示した設備の装置および方法論より安全ではない。恐らくこれは、“高い安全性”と“気密の安全性”との間の差であり、潜在的な用途の大部分にとってはあまり重要でない区別である。

【0099】

大域埋め込みコードを付けることができる紙、文書、プラスチック加工身分証明カード、および他の材料への印刷における使用

用語“信号”を、ディジタルデータ情報、オーディオ信号、画像、等を指示するためにしばしば狭義において使用する。“信号”のより広義の解釈と、より一般的に意図されたものとは、どの様な材料のどの様な形式の変化も含む。したがって、一般的な紙の断片のマイクロトポロギーは、信号（例えばｘ－ｙ座標の関数としての高さ）となる。プラスチックの平坦な断片の屈折特性は、（空間の関数としての）信号となる。要点は、写真感光乳剤、オーディオ信号、およびディジタル化情報は、本発明の原理を使用することができる信号の唯一の形式ではないということである。

【0100】

適切な場合として、ブライユ点字印刷機械に大変よく似た機械を、前記で概説した固有の´ノイズ状´検証を付けるように設計することができる。これらの検証を、ブライユ点字の形成において加えられるよりはるかに小さい圧力によって、そのパターンが書類の普通の使用者によって認められないような位置に加えることができる。しかし、本明細書のステップを続け、微細な検証の機構によってこれらを用いることによって、固有検証コードを、日常の便箋としての目的を意図したものや、重要な文書、法的な提出物、または他の保証された作品である、どのような紙面にも配置することができる。

【0101】

このような実施例における検証作品の読み取りは、一般的に、文書を光学的に種々の角度において単に読み取ることによって行われる。これは、紙面のマイクロトポロギを推論するために安価な方法となる。確かに紙のトポロギを読み取る他の形式も可能である。

【0102】

例えば運転免許書である身分証明カードのようなプラスチックに封入された作品の場合

において、同様のブライユ点字印刷機械に類似した機械を、固有検証コードを付けるのに利用することができる。感光材料の薄い層をプラスチックの内側に埋め込み、“感光”させることもできる。

【0103】

“ノイズ状”信号によって変調させることができる材料が存在するところならどこでも、この材料は、固有検証コードおよび本発明の原理を利用するための適切なキャリヤとなることは明らかである。経済的に検証情報を付加し、信号レベルを各々すべての用途がそれ自身に対して規定する許容しうるしきい値より下に保持する問題が残りの全てである。

【0104】

リアルタイムエンコーダ

実施例の第１の組は、画像または信号の符号化を行う標準的なマイクロプロセッサまたはコンピュータを最も一般に使用し、代表的なフォンノイマン型プロセッサより速くすることができるカスタム符号化装置を使用することができる。このようなシステムを、すべての様式のシリアルデータストリームに使用することができる。

【0105】

音楽およびビデオテープ記録を、シリアルデータストリーム、しばしば著作権侵害を受けるデータストリームの例とする。許可された記録を検証データによって符号化し、著作権侵害された盗品をこれらが形成されたものからオリジナルを探索できるようにしたならば、実施の試みの助けとなるであろう。

【0106】

著作権侵害は、本発明を必要とすることの１つにすぎない。他の事は、認証である。しばしば、データの所定の組が（しばしばその発生から数年後）実際に何を意図しているのかを確認することが重要になる。

【0107】

これらおよび他の必要性を説明するために、図５のシステム２００を使用することができる。システム２００を、検証符号化ブラックボックス２０２として考えることができる。システム２００は、（後に“マスタ”または“非符号化”信号と呼ばれる）入力信号およびコードワードを受け、検証符号化出力信号を（一般にリアルタイムで）発生する。（通常、本システムは、後の復号化に使用するキーデータを提供する）。

【0108】

“ブラックボックス”２０２の中身は、種々の形態をとることができる。典型的なブラックボックスシステムを図６に示し、これは、参照表２０４と、ディジタルノイズ源２０６と、第１および第２スケーラ２０８および２１０と、加算器／減算器２１２と、メモリ２１４と、レジスタ２１６とを含む。

【0109】

（図示した実施例においては、１０００００標本毎秒のレートにおいて供給される８－２０ビットデータ信号であるが、他の実施例においては、適切なＡ／ＤおよびＤ／Ａコンバータが設けられている場合、アナログ信号とすることができる）入力信号を、入力端子２１８から参照表２０４のアドレス入力端子２２０に供給する。各々の入力標本（すなわち、参照表アドレス）に対して、参照表は、対応する８ビットディジタル出力ワードを供給する。この出力ワードを、第１スケーラ２０８の第１入力端子に供給されるスケーリング係数として使用する。

【0110】

第１スケーラ２０８は、第２入力端子を有し、この入力端子にノイズ源２０６から８ビットディジタルノイズ信号を供給する。（図示した実施例において、ノイズ源２０６は、アナログノイズ源２２２およびアナログ－ディジタルコンバータ２２４を具えるが、再び、他の手段を使用することができる。）図示した実施例におけるノイズ源は、５０から１００のディジタル数（例えば、－７５から＋７５）の半値全幅（ＦＷＨＭ）を有する、ゼロ平均出力値を有する。

【0111】

第１スケーラ２０８は、その入力端子における２つの８ビットワード（スケール係数およびノイズ）を乗算し、システム入力信号の各々の標本に対して、１つの１６ビット出力ワードを発生する。ノイズ信号がゼロ平均値を有することから、第１スケーラの出力信号も同様にゼロ平均値を有する。

【0112】

第１スケーラ２０８の出力信号を、第２スケーラ２１０の入力端子に供給する。第２スケーラは、大域的スケーリング機能を行い、最終的に入力データ信号中に埋め込まれる検証信号の絶対量を確立する。前記スケーリング係数を、スケール制御装置２２６（簡単な加減抵抗器から、グラフィカルユーザインタフェースにおいて図式的に実現された制御まで、多くの形態をとることができる）によって設定し、別個の用途の要求にしたがって変更すべきこの係数を可能にする。第２スケーラ２１０は、その出力ライン２２８にスケールノイズ信号を発生する。このスケールノイズ信号の各々の標本を、メモリ２１４に順次記憶する。

【0113】

（図示した実施例において、第１スケーラ２０８からの出力信号は、－１５００と＋１５００（１０進数）との間で変化しうるが、第２スケーラ２１０からの出力信号は、小さい１つの数字である（－２と＋２との間のような））。

【0114】

レジスタ２１６は、多ビット検証コードワードを記憶する。図示した実施例において、このコードワードは、８ビットから成るが、より大きいコードワード（数１００ビットに及ぶ）が一般的に使用される。これらのビットを一度に１つ参照し、入力信号のスケールノイズ信号による変調の程度を制御する。

【0115】

特に、ポインタ２３０を、レジスタ２１６におけるコードワードのビット位置を通じて順次に循環させ、“０”または“１”の制御ビットを加算器／減算器２１２の制御入力端子２３２に供給する。ある入力信号標本に関して、制御ビットが“１”の場合、ライン２３２におけるスケールノイズ信号標本を入力信号標本に加算する。制御ビットが“０”の場合、スケールノイズ信号標本を入力信号標本から減算する。加算器／減算器２１２からの出力端子は、ブラックボックスの出力信号を発生する。

【0116】

コードワードのビットに従ったスケールノイズ信号の加算または減算は、一般にごく僅かな入力信号の変調に影響する。しかしながら、メモリ２１４の内容の認識によって、ユーザは、符号化を後に復号化し、オリジナル符号化処理において使用されるコード番号を決定することができる。（実際に、メモリ２１４の使用は、以下に説明するように任意である）。

【0117】

符号化信号を、印刷された画像に変換された形式、磁気媒体（フロッピーディスク、アナログまたはＤＡＴテープ、等）に記憶された形式、ＣＤ－ＲＯＭ、等々を含むよく知られた方法において配布することができることが認識されるだろう。

【0118】

復号化

種々の技術を、疑わしい信号が符号化されているままで検証コードを決定するのに使用することができる。２つを以下で論考する。第１のものは、多くの用途にとって後者よりも好適ではないが、ここで論考することによって、読み手は、本発明を理解するより完全な状況を得るであろう。

【0119】

さらに特に、第１の復号化方法は、差方法であり、オリジナル信号の対応する標本を疑わしい信号から減算し、差標本を得ることによるものであり、次に決定論的に符号化された証印（すなわち、記憶されたノイズデータ）に対して調査する。したがってこのアプローチを、“標本に基づく決定論的”復号化技術と呼ぶことができる。

【0120】
第２の復号化技術は、オリジナル信号を使用しない。個々の標本を調査して、予め決められたノイズ特性を探すこともしない。むしろ、疑わしい信号の統計値（またはこれらの一部）を、全体として考え、分析して、信号全体に充満する検証信号の存在を識別する。充満に対する言及は、検証コード全体を、疑わしい信号の小さい部分から識別することができることを意味する。したがってこの後者のアプローチを、“ホログラフィック統計的”復号化技術と呼ぶことができる。
【0121】
これらの方法の双方は、疑わしい信号をオリジナルに整合させることによって開始する。これは、スケーリング（例えば、振幅、継続時間、色バランス、等における）と、オリジナルの標本化レートを復旧するための標本化（または再標本化）とを必要とする。上述した実施例におけるように、この整合機能に関係する操作を行うことができる種々の良く理解された技術が存在する。
【0122】
言及したように、第１の復号化アプローチは、オリジナル信号を整合された疑わしい信号から減算し、差信号を残すことによって生じる。次に連続する差信号標本の極性を、対応する記憶されたノイズ標本信号の極性と比較し、検証コードを決定することができる。すなわち、第１差信号標本の極性が第１ノイズ信号標本の極性と一致した場合、検出コードの第１ビットを“１”とする。（このような場合、９番目、１７番目、２５番目、等の標本の極性も、すべて正とすべきである。）第１差信号標本の極性が、対応するノイズ信号標本の極性と反対である場合、検証コードの第１ビットを“０”とする。
【0123】
差信号の８つの連続する標本について前述の分析を行うことによって、オリジナルコードワードを具えるビットの配列を決定することができる。好適実施例におけるように、符号化中、ポインタ２３０が、コードワードを通じて一度に１ビット進み、第１ビットによって開始する場合、差信号の最初の８つの標本を分析し、８ビットコードワードの値を唯一決定することができる。
【0124】
ノイズの無い世界（ここで言っているノイズは、検証符号化に作用するノイズと無関係である）において、前述の分析は、常に正確な検証コードをもたらす。しかし、ノイズの無い世界においてのみ適合した処理は、実際は利用が制限される。
【0125】
（さらに、ノイズの無い状況における信号の正確な検証を、種々の他のより簡単な方法、例えば、チェックサム、すなわち、疑わしい信号およびオリジナル信号間の統計的不可能性一致、等によって処理することができる）。
【0126】
復号化においてノイズが引き起こす異常を、信号の大きな部分を分析することによって、ある程度まで、処理することができるが、このような異常は、処理の信頼性において実際的な上限を依然として設定する。さらに、直面しなければならない悪人は、常にランダムノイズより優しくない。むしろ、人間によって引き起こされる形式の改ざん、歪み、不正な操作、等が、益々選択される。これらのような場合において、検証の信頼性の所望の程度は、他のアプローチによってのみ達成される。
【0127】
現在好適なアプローチ（“ホログラフィック、統計的”復号化技術）は、疑わしい信号を特定のノイズデータ（代表的に、メモリ２１４に記憶されたデータ）と再結合し、結果として得られる信号のエントロピを分析することに頼っている。“エントロピ”を、その最も厳密な数学的定義において理解する必要はなく、単に、ランダム性（ノイズ、平坦性、雪状性、等）を記述する最も簡潔な言葉とする。
【0128】
大部分のシリアルデータ信号は、ランダムではない。すなわちある標本は、通常、隣接

する標本と、ある程度相関する。対照的に、代表的にノイズは、ランダムである。ランダム信号（例えば、ノイズ）を、非ランダム信号に加算した場合（またはこれから減算した場合）、結果として得られる信号のエントロピは、一般的に増加する。すなわち、結果として得られる信号は、元の信号よりもランダムな偏差を有する。これは、現在の符号化処理によって発生された符号化出力信号の場合であり、元の非符号化信号より大きいエントロピを有する。

【0129】

対照的に、ランダム信号の非ランダム信号への加算（またはこれからの減算）が、エントロピを減少させる場合、なんからの例外が発生する。好適な復号化処理を使用し、埋め込み検証コードを検出することが、この例外である。

【0130】

このエントロピに基づく復号化方法を十分に理解するために、８番目毎に同様の処理であるオリジナル復号化処理の特徴を強調することが第１の助けとなる。

【0131】

前記で論考した符号化処理において、ポインタ２３０は、コードワードを通じて、入力信号の各々の連続する標本毎に１ビット増分する。コードワードが８ビット長の場合、ポインタは、コードワード中の同じビット位置に８番目の標本毎に戻ってくる。このビットが“１”ならば、入力信号にノイズを加算し、このビットが“０”ならば、入力信号からノイズを減算する。したがってポインタ２３０の周期的な進行によって、符号化信号の８番目毎の標本は、特徴を共有し、ポインタ２３０によってアドレスされているコードワードのビットが“１”か“０”に応じて、これらをすべて、対応するノイズデータによって増加するか（反対でもよい）、これらをすべて減少する。

【0132】

この特徴を利用するために、エントロピに基づく復号化処理は、疑わしい信号の８ビット毎に、同様の方法で処理する。特に、疑わしい信号の１番目、９番目、１７番目、２５番目、等の標本に、メモリ２１４に記憶された対応するスケールのノイズ信号（すなわち、各々、１番目、９番目、１７番目、２５番目、等のメモリ位置に記憶されたノイズ信号）を加算することによって、処理は開始する。次に、結果として得られる信号（すなわち、８番目の標本毎に変更された疑わしい信号）のエントロピを計算する。

【0133】

（信号のエントロピまたはランダム性の計算法は、当業者には良く知られている。一般的に受け入れられているものは、各々の標本点において信号の導関数を取り、これらの値を二乗し、信号全体に渡って合計することである）。

【0134】

次に、上記のステップを繰り返し、この時、記憶されたノイズ値を、疑わしい信号の１番目、９番目、１７番目、２５番目、等の標本から減算する。

【0135】

これらの２つの操作の一方は、符号化処理を取消し、結果として得られる信号のエントロピを減少させ、他方は、それを悪化させる。メモリ２１４中のノイズデータの疑わしい信号への加算が、そのエントロピを減少させる場合、このデータは、以前オリジナル信号から減算されたに違いない。これは、ポインタ２３０が、これらの標本が符号化された時、“０”ビットを指していたことを示す。（加算器／減算器２１２の制御入力端子における“０”は、スケールノイズの入力信号からの減算を生じる）。

【0136】

反対に、ノイズデータの疑わしい信号の８番目毎の標本からの減算が、そのエントロピを減少させる場合、符号化処理は、以前このノイズを加算したに違いない。これは、ポインタ２３０が、標本１、９、１７、２５、等が符号化された時、“１”を指していたことを示す。エントロピの減少が、記憶されたノイズデータの疑わしい信号への／からの（ａ）加算または（ｂ）減算のいずれかによるものかに注目することによって、コードワードの第１ビットが、（ａ）“０”または（ｂ）“１”であるかを決定することができる。

【0137】
上記の操作を、疑わしい信号の第２標本（すなわち、２、１０、１８、２６．．．）に始まる一定の間隔をおいた標本のグループに対して行う。結果として得られる信号のエントロピは、コードワードの第２ビットが、“０”または“１”のいずれであるかを示す。疑わしい信号の続く６個のグループに対して同様に、コードワードの８ビットすべてを識別するまで繰り返す。
【0138】
上述したアプローチが、個々の標本の値を変更する改ざん機構に変動されないことは、理解されるであろう。すなわち、代わりに、このアプローチは、信号のエントロピを、結果における高い程度の信頼性を生じるものと見なす。さらに、信号のわずかな抜粋をこの方法によって分析し、オリジナル著作物の細部の著作権侵害も検出することができる。したがって結果として、疑わしい信号の自然および人的の改ざんの双方に直面して、統計的に健全である。
【0139】
さらに、このリアルタイムの実施例におけるＮビットコードワードの使用が、バッチ符号化システムに関連して、上述したのと類似の利益をもたらすことが理解されるだろう。（実際は、本実施例を、バッチ符号化システムにおいて、Ｎ個の差ノイズ信号を使用するものとして概念化することができる。第１ノイズ信号を、入力信号と同じ広がりを有し、標本間に０を有する１番目、９番目、１７番目、２５番目、等の標本（Ｎ＝８として）におけるスケールノイズ信号を具える信号とする。第２ノイズ信号を、標本間に０を有する２番目、１０番目、１８番目、２６番目、等の標本におけるスケールノイズ信号を具える同様の信号とする。その他同様。これらの信号をすべて混合し、複合ノイズ信号を発生する。）このようなシステムにおいて固有の重要な利点の１つは、一致が真に一致である統計的な信頼性（検証コードの各々の連続するビットとともに倍になる信頼性）の程度が高いことである。このシステムは、疑わしい信号の１つの決定論的な埋め込みコード信号に対する主観的な評価に頼らない。
【0140】
説明的な変形例
上述した説明から、示したシステムに対して、基本的な原理を変更することなく、多くの変更を行えることが認識されるだろう。これらの変形例のいくつかを、以下に記述する。
【0141】
上述した復号化処理は、どちらの操作がエントロピを減少させるのかを見つけるために、記憶されたノイズデータの疑わしい信号への／からの加算および減算の双方を試す。他の実施例において、これらの操作の一方のみを行う必要がある。例えば、ある一方の復号化処理において、疑わしい信号の８番目毎の標本に対応する記憶されたノイズデータを、前記標本に加算のみ行う。結果として得られる信号がそのために増加した場合、コードワードの対応するビットは、“１”である（すなわち、このノイズは、以前、復号化処理中に加算されており、再び加算されたために、信号のランダム性のみが増加した）。結果として得られる信号がそのために減少した場合、コードワードの対応するビットは、“０”である。記憶されたノイズ信号を減算するエントロピの他の試験は、必要ない。
【0142】
検証処理（符号化および復号化）の統計的信頼性を、大域的スケーリングファクタの適切な選択によって、どのような信頼性しきい値（例えば、９９．９％、９９．９９％、９９．９９９％、等）も実質的に越えるように設計することができる。なんらかの所定の用途（大部分の用途においては必要ない）における特別の信頼性を、復号化処理を再検査することによって達成することができる。
【0143】
復号化処理を再検査する一つの方法は、識別されたコードワードのビットに従って疑わしい信号から記憶されたノイズデータを除去し、“復旧”信号を発生する（例えば、コー

ドワードの第１ビットが“１”であることが分かった場合、メモリ２１４の第１、第９、第１７、等の位置に記憶されたノイズ標本を、疑わしい信号の対応する標本から減算する）ことである。記憶されたノイズ信号のエントロピを測定し、他の測定における基線として使用する。次に、この処理を繰り返し、この時、変更されたコードワードに従って、記憶されたノイズデータを疑わしい信号から除去する。変更されたコードワードは、結合された（例えば、第１）１ビットを除いて、識別されたコードワードと同一である。結果として得られる信号のエントロピを測定し、前記基線と比較する。識別されたコードワードにおけるビットのトグリングが増加されたエントロピを生じる場合、識別されたコードワードのそのビットの精度は、確実になる。トグルされた確認されたコードワードの異なったビット毎に、コードワードのすべてのビットが検査されるまで、この処理を繰り返す。各々の変更の結果として、基線値に比べてエントロピが増加する。

【0144】

メモリ２１４に記憶されたデータは、種々の二者択一を受ける。上述した論考において、メモリ２１４は、スケールノイズデータを含む。他の実施例において、非スケールノイズデータを、代わりに記憶することができる。

【0145】

さらに他の実施例において、入力信号それ自身の少なくとも一部を、メモリ２１４に記憶することが望ましいかもしれない。例えば、このメモリは、８つの署名ビットをノイズ標本に割り当て、１６ビットを１８または２０ビットオーディオ信号標本の最上位ビットの記憶に割り当てることができる。これは、いくつかの利益を有する。１つは、“疑わしい”信号の整合が簡単になることである。他の利益は、既に符号化された入力信号を符号化する場合、メモリ２１４内のデータを、どちらの符号化処理が最初に行われたかを識別するのに使用することができることである。すなわち、メモリ２１４内の入力信号データから（不十分にもかかわらず）、一般に、２つのコードワードのどちらが符号化されているかを決定することができる。

【0146】

メモリ２１４のさらに他の二者択一は、全体を省略できることである。

【0147】

これを達成できる方法の１つは、符号化処理において、既知の鍵番号によって種を蒔かれるアルゴリズム式ノイズ源のような決定論的ノイズ源を使用することである。同じ鍵番号によって種を蒔かれる同じ決定論的ノイズ源を、復号化処理において使用することができる。このような装置において、メモリ２１４に通常記憶される大きなデータセットの代わりに、後に復号化において使用するために鍵番号のみを記憶する必要がある。

【0148】

代わりに、符号化中加算されたノイズ信号がゼロ平均値を有しておらず、コードワード長さＮがデコーダにとって既知である場合、万能復号化処理を行うことができる。この処理は、上述した手順と同様のエントロピ試験を使用するが、可能なコードワードを循環し、試験されているコードワードのビットにしたがって、エントロピの減少が認められるまで、疑わしい信号のＮ番目の標本毎に小さいダミーノイズ値（例えば、予測される平均ノイズ値より小さい）を加算／減算する。しかしながら、このようなアプローチは、他の実施例より低い安全性しか示さない（例えば、野蛮な力によるクラッキングを受けやすい）ため、大部分の用途に対しては好適ではない。

【0149】

多くの用途を、異なったコードワードを使用し、各々が同じノイズデータを使用する、入力信号のいくつかの異なるように符号化された変形を発生する図７に示した実施例によって取り扱うことができる。さらに特に、図７の実施例２４０は、ノイズ源２０６からのノイズを、第１コードワードによる入力信号の識別符号化中に記憶するノイズストア２４２を含む。（図７のノイズ源を、図の便宜上、リアルタイムエンコーダ２０２の外側に示す。）その後、入力信号の追加の検証符号化販を、前記ストアから記憶されたノイズデータを読み取り、Ｎ番目のコードワードを通じて交互に結合し、この信号を符号化すること

によって発生することができる。（２値逐次コードワードを図７に示すが、他の実施例においてコードワードの任意の配列を使用することができる。）このような装置によって、比例したサイズのロングタームノイズメモリを必要とすることなく、多くの数の異なって符号化された信号を発生することができる。代わりに、一定量のノイズデータを記憶し、オリジナルを１回または１０００回符号化する。

【0150】

（もし望むなら、いくつかの異なって符号化された出力信号を、順次ではなく同時に発生することができる。あるこのような実施は、各々が同じ入力信号および同じスケールノイズ信号によって駆動されるが、異なったコードワードによって駆動される複数の加算器／減算器を含む。この時各々は、異なって符号化された出力信号を発生する）。

【0151】

同じオリジナルの多くの異なった符号化版を有する用途において、コードワードのすべてのビットを常に識別する必要はないことが認識されるだろう。例えば時々、用途は、疑わしい信号が属するコードのグループのみの検証を必要としてもよい。（例えば、コードワードの高次のビットは、同じソース作品のいくつかの異なった符号化版が発生された構造を示す低次のビットは、特定のコピーを示す。疑わしい信号が関係している構造を検証するために、構造を高次のビットのみによって検証することができることから、低次のビットを調査する必要はない。）検証必要条件を、疑わしい信号におけるコードワードビットの部分集合を識別することによって満たすことができるならば、復号化処理を短縮することができる。

【0152】

いくつかの用途を、あるときには異なったコードワードとともに、何回か積分作業中に、符号化処理を再開始することによって最適に取り扱うことができる。例として、ビデオテープ作品（例えば、テレビジョン番組）を考える。ビデオテープ作品の各々のフレームを、固有コード番号とともに検証符号化することができ、図８に示したのと同様の装置２４８によってリアルタイムで処理することができる。垂直帰線をシンク検出器２５０によって検出する度に、ノイズ源２０６をリセットし（例えば、丁度発生された配列を繰り返す）、検証コードを次の値に増加刷る。それによってビデオテープの各々のフレームは、固有に検証符号化される。代表的に、符号化信号を、長期間記憶するためにビデオテープに記憶する（レーザディスクを含む他の記憶媒体も使用することができる）。

【0153】

符号化装置に戻ると、示した実施例における参照表２０４は、入力データ信号の大振幅の標本は、小振幅入力標本ができるよりも高いレベルの符号化検証符号化を取り扱うことができるという事実を利用する。したがって例えば、０、１または２の１０進数値を有する入力データ標本を、１（またはゼロ）のスケール係数に対応させることができるが、２００を越える値を有する入力データ標本を、１５のスケール係数に対応させることができる。一般的に言って、スケール係数および入力標本値は、平方根関係によって対応する。すなわち、標本化入力信号の値における４つ折の増加は、これらに関係するスケール係数の値における２つ折の増加にほぼ対応する。

【0154】

（ゼロのスケーリング係数に対する挿話的参照として、例えば、ソース信号が時間的または空間的に情報内容が無い場合に言及する。画像において、例えば、いくつかの隣接した０の標本値によって特徴付けられる領域を、フレームの真黒領域に対応させることができる。ゼロのスケーリング値を、著作権侵害される画像データが実際的にないことから、ここに充てることができる）。

【0155】

符号化処理を続けると、当業者は、示した実施例における“レールエラー”に対するポテンシャルを認識するであろう。例えば、入力信号が８ビット標本から成り、これらの標本が０から２５５（１０進数）の範囲全体に及んでいる場合、入力信号への／からのスケールノイズの加算／減算は、８ビットによっては表すことができない出力信号（例えば、

－２または２５７）を発生するかもしれない。この状況を修正する多くの良く理解されている技術が存在し、これらのあるものは順行的であり、これらのあるものは反動的である。（これらの既知の技術は共通して、入力信号が０－４または２５１－２５５の範囲に標本を持たないようにし、それによってノイズ信号による変調を安全に行うか、他にレールエラーを発生する入力信号標本を検出し、適合するように変更する装置を含むかである）。

【0156】

示した実施例は、コードワードを逐次に、一度に１ビットずつ進むことを記述するが、コードワードのビットをこの目的のために順次ではなく使用できることが理解できるであろう。実際に、コードワードのビットを、なんらかの予め決められたアルゴリズムに従って選択することができる。

【0157】

入力信号の瞬間の値に基づくノイズ信号の動的なスケーリングは、多くの実施例において省略することができる最適化である。すなわち、参照表２０４および第１スケーラ２０８を完全に省略し、ディジタルノイズ源２０６からの信号を、加算器／減算器２１２に直接（または第２大域的スケーラ２１０を通して）供給することができる。

【0158】

さらに、ゼロ平均ノイズ源の使用が示した実施例を簡単にすることが認識されるであろうが、本発明には必要ではない。他の平均値を有するノイズ信号を、容易に使用することができ、（もし必要なら）Ｄ．Ｃ．補正を、本システム以外で行うことができる。

【0159】

ノイズ源２０６の使用も任意である。種々の他の信号源を、用途に応じて、制限（例えば、符号化検証信号が知覚できるようになるしきい値）に応じて使用することができる。多くの場合において、埋め込み検証信号のレベルは、検証信号がランダムな状況を有する必要がない、すなわちその性質にもかかわらず知覚できないほど十分に低い。しかしながら、埋め込み検証信号の知覚できないことのレベルに対して、最も大きな検証コード信号Ｓ／Ｎ比（この場合において、多少不適切な言葉）を提供するため、擬似ランダム源２０６が通常望ましい。

【0160】

検証符号化を、信号を（すなわち、米国著作権法の言葉において“実際の形式において一定の”）データとしての記憶された形式に減少した後で行う必要はないことが認識されるであろう。例えば、その演奏がしばしば不正に録音される人気音楽家の場合を考える。コンサートホールのスピーカを駆動する前にオーディオを検証符号化することによって、コンサートの認可されない録音を、個々の場所および時間まで追跡することができる。さらに、９１１非常呼び出しのような生のオーディオ源を、これらの後の認証を容易にするために、録音前に符号化することができる。

【0161】

ブラックボックス実施例を独立型ユニットとして記述したが、多くの道具／器具中に構成要素として統合できることが認識されるであろう。その１つは、検証コードを走査した出力データ中に埋め込むことができるスキャナである。（これらのコードを、単にこのデータが個々のスキャナによって発生されたことを記念するために取り扱うことができる）。他のものは、Ａｄｏｂｅ社、Ｍａｃｒｏｍｅｄｉａ社、Ｃｏｒｅｌ社、および同様の会社によって提供されている一般向けの描画／グラフィックス／アニメーション／ペイントプログラムのような創造的なソフトウェアにおけるものである。

【0162】

最後に、リアルタイムエンコーダ２０２を個々のハードウェアの実装の参照とともに説明したが、種々の他の実装を代わりに使用できることが認識されるであろう。いくつかは、他のハードウェア形態を利用する。他のものは、説明した機能ブロックのいくつかまたはすべてに対してソフトウエアルーチンを使用する。（これらのソフトウエアルーチンを、８０ｘ８６ＰＣ互換コンピュータ、ＲＩＳＣベースのワークステーション、等のような

多くの異なった一般的な目的のプログラム可能コンピュータにおいて実行することができる。

【0163】

ノイズ、擬似ノイズ、および最適化ノイズの形式

これまで、本明細書は、画像または信号全体に渡って情報の１ビットを搬送するのに適切な搬送波信号の種類の多くの例の幾つかとして、ガウスノイズ、“ホワイトノイズ”、および用途器具から直接発生されたノイズを仮定した。ある目標を達成するために、ノイズの“設計”特性において、さらに順向的にすることが可能である。ガウスまたは器具ノイズを使用する“設計”は、“絶対的”安全性のためにいくらか向けられている。本明細書のこの節では、検証情報の究極的な搬送波と考えることができるノイズ信号の設計のための、他の考察を調べる。

【0164】

いくつかの用途に関して、搬送波信号（例えば、第１実施例におけるＮ番目の埋め込みコード信号、第２実施例におけるスケールノイズデータ）を、検証信号にこの信号の知覚可能性に関してより絶対的な信号強度を与えるために設計することが有利であるかもしれない。ある例は、以下のようなものである。真のガウスノイズは、値“０”が最も頻繁に生じ、次に１および－１が各々等しい確率だが“０”よりは低い確率で生じ、次に２および－２、等々である。明らかに、値０は、本発明において使用されるような情報を搬送しない。したがって、ある簡単な調節または設計は、埋め込みコード信号の発生においてゼロが発生するときはいつも、新たな処理が引き継ぎ、値を“ランダムに”１または－１のいずれかに変換する。このような処理のヒストグラムは、０の値が空であり、１および－１の値が通常の０の値のヒストグラム値の半分だけ増加していることを除けば、ガウス／ポアソン型分布として現れる。

【0165】

この場合において、検証信号エネルギは、通常、信号のすべての部分において現れる。交換のいくつかは、“決定論的成分”がノイズ信号の発生の一部であるコードの安全性の（大抵、無視できる）低下が存在することを含む。これを完全に無視できる理由は、我々が、１または－１をランダムに選択するコイン投げ形式の状況を依然として準備しているからである。他の交換は、設計されたノイズのこの形式が、知覚可能性の高いしきい値を有し、データストリームまたは画像の最下位ビットが題材の商業上価値に関してすでに無視できる、すなわち、最下位ビットが信号（またはすべての信号標本）から取り除かれた場合、誰もその差を識別できず、題材の価値が損害を受けない用途にのみ使用することができることである。上述した例におけるこのゼロ値の制限は、当業者の誰もが実現できるような信号搬送波のノイズ特性を“最適化”する多くの方法の１つである。我々は、これを、自然ノイズを予め決められた方法においてすべての意図および目的に対してノイズとして読み取られる信号に変換することができるという意味で“擬似ノイズ”とも呼ぶ。暗号化方法およびアルゴリズムが、完全にランダムとして知覚される信号を、容易に、そしてしばしば定義によって生成することもできる。したがって、“ノイズ”という言葉は、観察者または聴取者によって主観的に定義されるものと、数学的に定義されるものとの間で、異なった意味を有する。後者の違いは、数学的ノイズが、異なった安全性の性質を有し、追跡することができる簡単さか、このノイズの存在を“自動的に認識”することができる簡単さかを有する。

【0166】

“万能”埋め込みコード

本明細書の大部分は、絶対的安全性のために、検証信号の情報のビットを搬送するノイズ様埋め込みコードを、各々すべての埋め込み信号に対して固有のものにすべきであるか、わずかに制限を少なくして、埋め込みコード信号を、例えばフィルムの１０００個の断片の１組に対して同じ埋め込みコードを使用するように控えめに発生すべきであることを教えている。いずれにせよ、我々が“万能”埋め込みコード信号と呼ぶことができるものを使用することによって、この技術に関して新たな用途を大きく開発することができる他

のアプローチが存在する。これらを使用することの経済性は、これらの万能コードの実際の低い信頼性（例えば、これらは、時間に頼った暗号復号化方法によって分析可能であり、したがって、可能的に妨げられるまたは置き換えられる）が、意図された使用を規定した場合の経済的利益と比較して経済的に無視できるようなものである。著作権侵害および非合法な使用は、単に、予測しうる“費用”および未徴収の収入源となり、すなわち全体の経済的分析における簡単なラインアイテムとなる。これの良い類似は、ケーブル産業とビデオ信号の波長を変えることとにおけるものである。一般に法律を甘受する市民である狡猾な技術的に熟練した個人が、全ての有料チャンネルをただにするためのケーブル接続ボックスにおいて、梯子をのぼり、数本のワイアをはじくことができることを誰もが知っていると思われる。ケーブル産業は、これを知っており、それを停止し、捕らえられたこれらを起訴する有効な方法を選択するが、この習慣に発する“失われた収入”は、いまだ普及しており、しかしシステム全体をスクランブルことによって得られる利益の割合としては、ほとんど無視できる。全体としてのスクランブル化システムは、“完全な安全性”の欠落にも係わらず、経済的に成功している。

【0167】

同様なことが、この技術の用途に対して真実であり、ある程度の安全性を低下する価格に対して、大きな経済的機会をそれ自身に与える。この節は、最初に、万能コードによって何がもたらされるかを記述し、次に、これらのコードを用いることができるいくつかの興味深い使用に移る。

【0168】

万能埋め込みコードを一般に、正確なコードの知識を配布することができるという概念に適用する。埋め込みコードを、（本明細書の他の部分において言及したように）訴訟がなされるまで決して接触されない秘密の金庫中に置かずに、代わりにその場で分析を行うことができる種々の場所に配布する。一般にこの配布は、安全性が制御された状況に依然として置かれており、ステップは、コードの認識が知ることを必要とするこれらに対して制限されることを意味する。著作権を有する作品を自動的に検出しようとする方法は、コードを知ることを必要とする“何か”の人間でない例である。

【0169】

万能コードの概念を実施する多くの方法が存在し、これらの各々が、何らかの所定の用途に関しては利点を有する。この技術を教える目的のために、我々は、これらのアプローチを３つのカテゴリー、すなわち、ライブラリを基礎とする万能コードと、決定論的公式を基礎とする万能コードと、予め規定された業界標準パターンを基礎とする万能コードとに分類する。おおざっぱなやり方は、第１のものは、後者の２つより安全性が高いが、後者の２つは、第１のものよりもより経済的に実現できるとする。

【0170】

万能コード：１）万能コードのライブラリ

万能コードのライブラリの使用は、個々の埋め込みコード信号の制限された組のみが発生し、どのような所定の符号化材料もこの制限された“万能コード”の部分集合を使用することを除いて、本発明の技術を使用することを単に意味する。一例は、以下のものが適切である。写真印画紙製造業者は、固有検証コードとともに販売したい８×１０インチの印画紙のすべてを前露光することを望むことができる。彼らは、検証コード認識ソフトウェアを、彼らの大口顧客、サービス部、在庫代理店、および個々の写真家に販売し、その結果、すべてのこれらの人々が、かれらの題材が正確にマークされていることを照合できるだけでなく、彼らがまさに得ようとしている第三者の題材がこの技術によって著作権を取得しているとして確認された場合、決定することができるようにすることも望む。この後者の情報は、多くの他の利益のなかで、著作権所有者を確認し、訴訟を無効にするのを助ける。この計画を“経済的に”行うために、各々すべての印画紙に固有検証埋め込みコードを発生することは、情報とは独立に数テラバイトを発生し、これらのバイトを記憶する必要があり、これらのバイトに認識ソフトウェアがアクセスする必要がある。代わりに、彼らは、５０個の独立“万能”埋め込みコード信号のみの組から得た１６ビット検証コ

ードを彼らの印画紙に埋め込むことを決める。これをどのように行うかについての詳細は、次の節におけるものであるが、かれらの認識ソフトウェアが、代表的に８×１０の印画紙上に広げられた５０×１６の個々の埋め込みコードに対して（ディジタル圧縮を考慮して）１メガバイトから１０メガバイトの情報である、彼らのコードのライブラリにおける埋め込みコードの制限された組を含むことのみを必要とすることが、ここでの要点である。１６の代わりに５０を選ぶ理由は、安全性がわずかに増すためであり、すべての写真に対して同じ１６個の埋め込みコードにした場合、シリアル番号容量が2の１６乗に制限されるだけでなく、より少ない洗練された著作権侵害者が、これらのコードを解読し、ソフトウエアツールを使用してこれらを除去することができる。

【0171】

この計画を実施するための多くの異なった方法が存在し、以下は好適な方法の１つである。企業経営の知識によって、埋め込みコード信号のための１インチ当たり３００画素の規準は、多くの用途に関して十分な解像度であると定義される。これは、復号埋め込みコード画像が、８×１０のシート上に極めて低いレベルにおいて露光すべき３０００×２４００画素を含むことを意味する。これは、７２００００画素を与える。図５および６のブラックボックス手段において記述したような我々の交互配列符号化システムを使用すれば、各々の独立埋め込みコード信号は、１６分の７２００００すなわち４５０ｋ程度の真の情報を搬送する画素、すなわち所定のラスタライン上のすべての１６番目の画素のみを含む。これらの値は、代表的に2から－2の範囲のディジタル数であり、符号３ビット数によって十分に記述される。このとき埋め込みコードの未加工の情報内容は、４５０ｋの３／８番目のバイト倍すなわち１７０キロバイト程度である。ディジタル圧縮によって、これをさらに減少することができる。これらの決定のすべては、近い将来になんらかの所定の用途によって規定される、本技術分野において既知の、標準工学最適化原理に属する。したがって、我々は、これらの５０個の独立埋め込みコードが数メガバイトに達することが分かる。これは、認識ソフトウェア内の万能コードの“ライブラリ”として配布するのに全く適度なレベルである。進歩した標準暗号化装置を、自称著作権侵害者が単に万能埋め込みコードをリバースエンジニアするために認識ソフトウェアを購入したことに１つが関係する場合、これらのコードの正確な特徴を隠すために使用することができる。認識ソフトウェアは、本明細書において教えた認識技術を用いる前に、コードを簡単に復号化することができる。

【0172】

認識ソフトウェアそれ自体は、種々の特徴を確かに有するが、行う中心的な仕事は、所定の画像中にある万能著作権コードが存在する場合、これを決定することである。鍵となる問題は、もしあるとすれば、合計５０個の万能コードのうちどの１６個が含まれているかということと、１６個が見つかった場合、これらのビット値は何かということとである。これらの問題の回答の決定における鍵変数は、整合と、回転と、拡大（スケール）と、範囲とである。助けとなるヒントが何もない大部分の一般的な場合において、すべての変数を、すべての相互結合に渡って独立して変化させるべきであり、５０個の万能コードの各々を、エントロピの減少が発生するかどうかを見つけるために、加算および減算によって検査すべきである。厳密に言えば、これは莫大な仕事であるが、疑わしいコピーと比較するオリジナル画像を有するような、または８×１０の印画紙に比例する画像のオリエンテーションおよび範囲を知ることのような、この仕事をはるかに簡単にする多くの有用なヒントが見つかり、簡単な整合技術によって、ある許容しうる程度に対する変数のすべてを決定することができる。このとき、エントロピにおけるなんらかの減少を見つけるために、５０個の万能コードを通して繰り返すことが単に必要である。１つを行った場合、他の１５個も行うべきである。５０個の万能コードの所定の順序を、ＩＤコードワードの最上位ビットから最下位ビットまでの順序に変換する設定をするために、プロトコルが必要である。したがって、我々が、万能コード番号“４”の存在を発見し、そのビット値が“０”であることを発見し、万能コード“１”から“３”が明確に存在しないことを発見した場合、我々のＮビットＩＤコード数の最上位ビットは“０”である。同様に、我々が、

次の存在する最も低い万能コードが番号“７”であることを見つけ、それが“１”であることが分かった場合、我々の次の最上位ビットは“１”である。適切に行うと、このシステムは、印画紙在庫シリアル番号を、ある登録または印画紙自体の製造業者に登録している限り、著作権所有者まで明確に追跡することができる。すなわち、我々は、万能埋め込みコード４、７、１１、１２、１５、１９、２１、２６、２７、２８、３４、３５、３７、３８、４０、および４８を使用し、埋め込みコード０１１０　０１０１　０１１１　０１００を有する印画紙が、カナダ在住の未知の野性動物写真家兼、氷河映画撮影技師であるＬｅｏｎａｒｄ　ｄｅ　Ｂｏｔｉｃｅｌｌｉの所有物であるという登録を調べる。彼が無税で登録した彼のフィルムおよび印画紙の在庫を、彼がこの在庫を購入したとき、馬鹿げた簡単なプロセスを行う“郵便の必要がない”製造会社が親切にも準備した封筒に入れる、数秒の仕事のため、我々はこれを知っている。Ｌｅｏｎａｒｄに著作権使用料を支払う必要がある誰かは、それが現れることをチェックし、確実に登録は、著作権使用料の支払いプロセスをそのサービスの一部として自動化する。

【0173】

ある終点は、真に洗練された著作権侵害者と、違法の目的を持った他の者とが、種々の暗号化方法を実際に使用してこれらの万能コードを解読することができ、これらを販売し、コードを除去または歪ませるのを助けることができるソフトウェアおよびハードウエアツールを制作することである。しかしながら我々は、これらの方法を、本明細書の一部として教えない。とにかく、これは、万能コードの容易さとこれらが開く用途に支払う必要がある値段の１つである。

【0174】

万能コード：２）決定論的公式を基礎とする万能コード

万能コードのライブラリは、万能コードを付けられている信号および画像の存在および身元を開く鍵としての数メガバイトの独立した一般的にランダムのデータを記憶および変換することを必要とする。代わりに、種々の決定論的公式を、ランダムデータ／画像フレームの発生に使用し、これらによって、これらのコードのすべてをメモリ内に記憶することと、“５０個”の万能コードの各々に質問することとを回避することができる。決定論的公式は、所定の信号または画像中に存在することが一度知られているＩＤコードを決定する処理を高速化するのを助けることもできる。他方では、決定論的公式を、あまり洗練されていない著作権侵害者によって追跡することができる。一度追跡されると、これらを、インターネット上で１００個のニュースグループに掲示するように、より簡単に伝達することができる。これらは、追跡および公表をかまわない多くの用途には適切であり、独立万能埋め込みコードを発生する決定論的公式を、単にチケットとすることができる。

【0175】

万能コード：３）“簡単な”万能コード

この分類は、はじめの２つを結合したものの一部であり、この技術の原理の真に大きな規模の実施に最大限向けたものである。この種類を使用する用途は、信頼できる安全性が、低費用で大きな規模の実施と、これが可能にする莫大な経済的利益とほどは重要ではない形式のものである。一例としての用途は、検証認識ユニットを適度に値付けされた（テレビジョンのような）家庭用オーディオおよびビデオ装置中に直接配置する。このような認識ユニットは、代表的に、オーディオおよび／またはビデオを監視してこれらの著作権検証コードを探し、そこから、記録可能性が与えられているか否か、または中央オーディオ／ビデオサービス提供者に伝送されるとともに毎月の送り状に配置される番組特定課金メータの増加のような判断に基づく簡単な決定を行う。さらに、バーおよび他の公共の場所における“ブラックボックス”が、著作権を持った題材を監視し（マイクロフォンによって聞き）、ＡＳＣＡＰ、ＢＭＩ、等によって使用される詳細な報告書を生成することができる。

【0176】

簡単な万能コードの中心となる原理は、いくつかの基本的な業界標準の“ノイズ状”で継ぎ目のない繰り返しのパターンを、信号、画像、および画像列中に挿入し、安価な認識

ユニットが、Ａ）著作権“フラグ”の存在を決定するか、Ｂ）Ａに追加して、より複雑な決定構成および動作を容易にすることができるようにすることである。

【0177】

本発明のこの実施例を実現するために、独立埋め込みノイズ信号を発生する基本的な原理を、安価な認識信号処理ユニットに適応させると同時に、有効なランダム性およびホログラフィックの浸透の性質を維持するために、簡単にする必要がある。これらの簡単なコードの大規模産業への採用によって、コード自体は公有情報と隣接し（ケーブルスクランブリングボックスがほとんど事実上の公有であるように）、ブラックマーケット対策を開発するために確定された著作権侵害者に対してドアを開いたままであるが、この状況は、ケーブルビデオのスクランブル化や、このような違法活動の客観的経済的分析とまったく類似している。

【0178】

順向の著作権検出のこの一般的な領域における本出願人に既知のある先行技術は、オーディオ業界における多くの会社によって採用されたシリアルコピー管理システムである。本出願人の知っている限り、このシステムは、オーディオデータストリームの一部ではないが、それにもかかわらずオーディオストリームに挿入され、関連するオーディオデータを複製すべきか否かを示すことができる、非オーディオ“フラグ”信号を使用する。このシステムが有する１つの問題は、この追加の“フラグ”信号をサポートすることができる媒体および装置が制限されることである。他の欠陥は、フラグシステムが、より複雑な決定を行うのに使用できる身元情報を搬送しないことである。さらに他の困難は、アナログ信号の高品質なオーディオ標本化が、あるディジタルマスタの完全なディジタルコピーを任意に近く行えるようになる恐れがあり、この可能性を禁じる対策は、無いように思われる。

【0179】

本発明の原理を、オーディオ用途、ビデオ、および上述した他のすべての用途における、これらのおよび他の問題を影響を与えることができる。簡単な万能コードの用途の一例は、以下のようなものである。ある１つの業界標準“１．０００００秒のノイズ”は、なんらかの所定のオーディオ信号の著作権符号の存在または不在を示す最も基本的なものとして規定される。図９は、業界標準ノイズ秒が時間領域４００および周波数領域４０２の双方においてどのように見えるかの一例である。定義によって、連続関数であり、標本化レートおよびビット量子化の何らかの組み合わせに適合する。規格化された振幅を有し、どのようなディジタル信号振幅にも任意に尺度合わせすることができる。この信号の信号レベルおよび最初のM番目の導関数は、２つの境界４０４において連続であり（図９ＣＣ）、その結果、繰り返す場合、信号における“不連続”は（波形として）目に見えない、または、ハイエンドオーディオシステムによって演奏される場合、聞き取れない。１秒の選択は、この例において任意であり、この間隔の正確な長さを、可聴性、擬似ホワイトノイズ状態、継ぎ目のない繰り返し可能性、認識処理の容易さ、および著作権を付ける決定を行えることによる速度のような理由から得る。この繰り返しノイズ信号の信号または画像への（再び、人間の知覚力以下のレベルにおける）挿入は、著作権題材の存在を示す。これは、本質的に１ビット検証コードであり、他の検証情報の埋め込みを、この節において後に論考する。この検証技術の使用を、ここで論考した低価格家庭向け器具を遙に越えて拡張することができ、スタジオにこの技術を使用することができ、監視局を設定し、実際に数１００チャネルの情報を同時に監視し、マークされた信号ストリームを探索し、さらに、課金ネットワークおよび印税追跡システムに適合する関連する身元コードを探索することができる。この基本的な標準化ノイズ署名を、継ぎ目無く何度も繰り返し、基本著作権検証をマークすべきオーディオ信号に加える。“簡単”という言葉の理由の一部は、以下のように理解される。明らかに著作権侵害者は、この業界標準信号について知るであろうが、削除または改ざんのようなこの知識から得られる彼らの違法な使用は、大規模な市場に対する全体的な技術の経済的な価値に比較して、経済的に非常に小さいものとなる。大部分のハイエンドオーディオに関して、この信号を、フルスケールから８０から１

００ｄＢ低下またはさらに小さいものとし、各々の状況を、たとえ推薦されるものが確実に存在しても、それら自身のレベルに選択することができる。信号の振幅を、ノイズ署名が用いられているオーディオ信号レベルに従って変調することができる。すなわちこの振幅を、ドラムビートの場合、意味のある程度、しかし聞き取れるまたは不快になるほど劇的ではない程度に増加することができる。これらの程度は、記述すべき認識回路網を単に助ける。

【0180】

このノイズ信号の存在の低価格な機器による認識を、種々の方法において行うことができる。あるものは、オーディオ信号出力の測定の簡単な原理に対する基本的な変形に基づいている。ソフトウェア認識プログラムを書くことができ、さらに洗練された数学的検出アルゴリズムを、より高い信頼性のある検証の検出を行うために用いることもできる。このような実施例において、著作権ノイズ署名の検出は、オーディオ信号の時間平均された出力レベルと、ノイズ署名を減算した同じオーディオ信号の時間平均された出力レベルとの比較を含む。ノイズ信号を減算されたオーディオ信号が、変更されていないオーディオ信号より低い出力レベルを有する場合、著作権署名が存在し、同じ意味で、ある状態フラグを設定する必要がある。この比較の実行において含まれる主な工学的に微妙なものは、オーディオの録音再生速度が不一致（例えば、ある機器は、正確に１秒間隔に関して０．５％“遅い”かもしれない）である処理と、何らかの所定のオーディオ中の一秒のノイズ署名の未知の位相の処理（基本的に、この“位相”は、０から１秒位までかもしれない）とを含む。上述した２つほど中心的なものではないがそれにもかかわらず説明すべき他の微妙なものは、認識回路が、オーディオ信号に元に埋め込まれたノイズ署名より大きい振幅のノイズ署名を減算すべきではないことである。幸運にも、これを、単に小さい振幅のノイズ信号のみを減算することによって実行することができ、出力レベルが低下した場合、これは、出力レベルにおける“谷に向かっている”しるしとなる。さらに他の関連する微妙なものは、出力レベルの変化が、全体の出力レベルに対して極めて小さく、計算を一般に適切なビット精度によって、例えば、時間平均された出力レベルにおいて１６－２０ビットオーディオにおいて、３２ビット値演算および集積によって行う必要があることである。

【0181】

明らかに、低価格用途用のこの出力レベル比較処理回路を設計し組み立てることは、技術的最適化の仕事である。ある交換は、より低い価格と複雑さのために回路網に形成することができる“近道”に関する検証の実行における精度である。この認識回路網の機器内の配置の好適実施例は、その仕事用に注文生産した１つのプログラム可能集積回路によるものである。図１０は、あるこのような集積回路５０６を示す。ここで、オーディオ信号が、ディジタル信号として、またはＩＣ５００内でディジタル化すべきアナログ信号として５００中に入り、出力信号は、著作権ノイズ署名が見つかった場合にあるレベルに設定され、見つからなかった場合に他のレベルに設定されるフラグ５０２である。標準化ノイズ署名波形を、ＩＣ５０６内の読み出し専用メモリ５０４に記憶することも示す。オーディオ信号のＩＣ５０６への適用と、有効なフラグ５０２の出力との間には、認識を行える前に、オーディオのある有限の位置を監視する必要があるため、僅かな時間遅延が存在する。この場合において、著作権ノイズ署名の存在または不在の正確な決定を行うために十分な時間を有する場合、ＩＣが外界に知らせる“フラグ有効”出力信号が必要になるかもしれない。

【0182】

図１０のＩＣ５０６の基本的な機能を実行するのに用いられる特定の設計および設計の哲学の広い範囲の変形例が存在する。オーディオ技術者およびディジタル信号処理技術者は、いくつかの基本的に異なった設計を生成することができる。あるこのような設計を図１１において、それ自体は、後に論考するような他の技術的最適化に属する処理５９９によって示す。図１１は、アナログ信号処理ネットワーク、ディジタル信号処理ネットワーク、またはソフトウェアプログラムのプログラミングステップのいずれかのフローチャー

トを示す。我々は、ある経路に沿った入力信号６００を、時間平均パワーメータ６０２に供給し、結果として得られるパワー出力それ自体を、信号P_{sig}として扱うことに気づく。右上に対して、我々は、６０４で通常速度の１２５％において読み取られ、したがってそのピッチが変化し、６０６で“ピッチ変化ノイズ信号”を示す、標準ノイズ署名５０４を見つける。次に、ステップ６０８において入力信号からこのピッチ変化ノイズ信号を減算し、この新たな信号を、６０２において示したのと同じ形式のここでは６１０で示す時間平均パワーメータに供給する。この操作の出力信号も、ここでは６１０でP_{s-pcn}と示す時間基準信号である。次にステップ６１２でパワー信号６１０からパワー信号６０２を減算し、パワー差信号P_{out}　６１３を生じる。万能標準ノイズ署名が、入力オーディオ信号６００において実際に存在する場合、ケース２、６１８、が発生し、４秒間程度のビート信号が、出力信号６１３において現れ、図１２、６２２のようなステップによってこのビート信号を検出しなければならない。ケース１、６１４は、周期的なビートが見られない一様なノイズ信号である。ステップ６０４における１２５％を、ここでは任意に選択しており、技術的な理由が最適値を決定し、異なったビート信号周波数６１８を導く。この例における４秒の待機は、事実上一定期間であるが、特に少なくとも２つまたは3つのビートを検出したい場合、図１２は、図１１の基本設計を、隣から０．０５秒遅延されたオーディオの部分において各々一斉に動作する２０個の並列回路によって１／２０秒程度遅延された入力信号の種々の遅延されたバージョンにどのように繰り返し作用させるかの概要である。この方法において、ビート信号が、１／５秒程度毎に見られ、ビート検出回路の列を下る進行波のように見える。この進行ビート波の存在または不在は、検出フラグ５０２をトリガする。同時に、例えば、少なくとも２秒のオーディオが、フラグ有効信号５０８を設定する前に聞こえることを保証するオーディオ信号モニタが存在する。

【0183】

オーディオの例を記述してきたが、ある繰り返し万能ノイズ信号または画像の同様の形式の定義を、多くの他の信号、画像、写真、およびすでに論考した物理的媒体に用いることができることは、当業者には明白であろう。

【0184】

上述したケースは、情報の１ビット面のみを取り扱った。すなわち、ノイズ署名信号を、存在するか（１）、しないか（０）とした。多くの用途に関して、さらに複雑な判定か、または課金明細書におけるログ情報等に使用することができるシリアル番号情報をさらに検出することが好ましい。上述したのと同様の原理を用いるが、ここでは、図９に示すようなＮ個の独立ノイズ署名が、１つのこのような署名の代わりに存在する。代表的に、あるこのような署名は、これによって著作権マーキングが単に存在することを検出するマスタとし、これは一般に他のものより大きいパワーを有し、次に他のより小さいパワーの“検証”ノイズ署名をオーディオに埋め込む。認証回路は、一度主要なノイズ署名の存在を見つけると、他のＮ個のノイズ署名に進み、上述したものと同様のステップを用いる。ビート信号が検出される場合、これは１のビット値を示し、ビート信号が検出されない場合、これは０のビット値を示す。代表的にＮを３２とし、2^{32}個の検証コードを、本発明を使用する何らかの所定の産業に対して利用できるようにすることができる。

【0185】

検証コードの長さが１である場合のこの技術の使用

本発明の原理を、１つの検証信号－－もし望むなら指紋－－の存在または不在のみを使用し、ある信号または画像が著作権を与えられていることの信頼性を与える場合において、明らかに適用することができる。業界標準ノイズ署名の上述した例は、ある適切な場合である。我々は、もはやコイン投げとの類似性の追加の信頼性を持たず、我々は、もはや追跡コード容量または基本シリアル番号容量を持たないが、多くの用途は、これらの属性を必要としないであろうし、１つの指紋による追加の簡単さは、なんらかの事象におけるこれらの他の属性を補って余りある。

【0186】

“壁紙”との類似性

“ホログラフィック”という言葉を、本明細書において、どのように検証コード番号を大部分完全な形態において符号化信号または画像全体に分布させるかを記述するのに使用してきた。これを、信号または画像の何らかの所定の断片は、完全な固有検証コード番号を含むという概念にも適用する。ホログラフィの物理的な実施の場合、この特性を失い始める前に、断片をどの位小さくできるかにおいて制限があり、ここでホログラフィック媒体の分解能制限は、ホログラフ自体に関する主要な要素である。図５の符号化装置を使用し、ゼロがランダムに１または－１に変化する上述した我々の“設計されたノイズ”をさらに使用する非改ざん配布信号の場合において、必要な断片の程度は、信号または画像ラスタラインにおいて単にＮ個の連続的な標本であり、ここでＮを、予め規定した我々の検証コード番号の長さであるとする。これは、情報の量であり、すなわち、ノイズおよび改ざんが作用する実際的な状況は、一般にこの簡単な数Ｎより１、２、または以上大きい桁の標本を必要とする。当業者は、これによって検証を行うことができる最も小さい断片の寸法における正確な統計の明確な定義に含まれる多くの変形が存在することを認識するであろう。

【0187】

教授の目的のために、本出願人は、固有検証コード番号を、画像（または信号）を横切って“壁紙貼りした”というアナロジも使用する。すなわち、画像全体に何度も繰り返す。ＩＤコード番号のこの繰り返しを、図５のエンコーダの使用におけるように定期的にすることができ、またはそれ自身ランダムにすることができ、図６のＩＤコード２１６のビットは、通常の繰り返し方法において停止せず、各々の標本においてランダムに選択され、このランダムな選択は、出力信号２２８の値とともに記憶される。とにかく、ＩＤコードの情報キャリヤ、独立埋め込みコード信号は、画像または信号を横切って変化する。したがって、壁紙との類似性を要約すると、ＩＤコード自体を何度も繰り返すが、各々の繰り返しがつけるパターンは、一般に追跡できない鍵に従って、ランダムに変化する。

【0188】

損失データ圧縮

上述したように、好適実施例の検証符号化は、損失データ圧縮およびその後の伸長とに耐えうる。このような圧縮は、特にディジタル化された娯楽番組（映画、等）のような状況における使用が益々増えると思われる。

【0189】

本発明の好適実施例によって符号化されたデータは、出願人に既知のすべての形式の損失圧縮に耐えうるが、商業的に最も重要だと思われるものは、ＣＣＩＴＴ　Ｇ３、ＣＣＩＴＴ　Ｇ４、ＪＰＥＧ、ＭＰＥＧおよびＪＢＩＧ圧縮／伸長標準である。ＣＣＩＴＴ標準は、黒および白の文書の圧縮（例えば、ファクシミリおよび文書記憶）において広く使用されている。ＪＰＥＧは、静止画に最も広く使用されている。ＭＰＥＧは、動画に最も広く使用されている。ＪＢＩＧは、黒および白の像への使用に関して、ＣＣＩＴＴ標準の有望な後継者である。これらのような技術は、損失データ圧縮の分野において良く知られており、良い概略を、Pennebaker et al, JPEG, Still Image Data Compression Standard, Van Nostrand Reinhold, N.Y., 1993において見ることができる。

【0190】

ステガノグラフィおよび、より複雑なメッセージまたは情報の伝送におけるこの技術の使用

本明細書は、信号全体に１つの検証コードの壁紙貼りと前記において呼んだものに集中する。これは、多くの用途に関して所望の特徴であると思われる。しかしながら、メッセージを通過させる、または適切な検証情報の極めて長い列を信号または画像中に埋め込むことが望ましい他の用途が存在する。多くのこれらの考えられる用途の１つは、所定の信号または画像がいくつかの異なったグループによって操作されることを意図され、画像の特定の領域が、各々のグループの適切な操作情報の検証および挿入に確保されている場合である。

【0191】

これらの場合において、図６におけるコードワード２１６を、ある予め決められた方法において、信号または情報位置の関数として実際に変化させることができる。例えば、画像において、コードをディジタル画像の各々すべてのラスタラインに関して変更することができる。１６ビットコードワードを２１６とすることができるが、各々の走査ラインは新たなコードワードを有し、したがって４８０の走査ライン画像は９８０バイト（４８０×２バイト）メッセージを通過させることができる。メッセージの受信者は、メモリ２１４に記憶されたノイズ信号にアクセスするか、使用されている符号化方法のノイズコードの万能コード構造を知る必要がある。本出願人の知る限り、これは、ステガノグラフィの成熟した領域の新規のアプローチである。

【0192】

万能コードの前述の３つの用途のすべてにおいて、万能コードに加えて、短い（ひょっとすると８または１６ビット）秘密コードを追加することがしばしば望まれる。これは、洗練された著作権侵害者による万能コードの削除の可能性に対する他の僅かな量の安全性をユーザにもたらす。

【0193】

本願人の先行出願

この点に対する詳細な説明は、ＰＣＴ国際公開パンフレットＷＯ９５／１４２８９号として公開されている本願人の先行国際出願の開示を単に繰り返した。上記単なる繰り返しは、以下の開示に対する背景を与える。

【0194】

Ｎ個の独立した埋め込みコード信号からの区別としての１つのマスタコード信号

ひょっとするとリアルタイムエンコーダの部分において例示されるこの開示のある部分において、Ｎ個の独立したソース信号同一空間埋め込み信号を、なにか所定の埋め込みコード信号の非ゼロ要素がその埋め込みコード信号に対して固有になるように設計する節約ステップを行った。より慎重に、所定の信号のある画素／標本点を、我々のＮビット識別ワードにおけるある予め決められたｍ番目のビット位置に“割り当てる”。さらに、かつ実現化の他の基本的な最適化として、すべてのＮの埋め込みコード信号に渡るこれらの割り当てられた画素／標本の集合は、正確に前記ソース信号の範囲であり、ソース信号における各々のそしてすべての画素／標本位置が、我々のＮビット識別ワードにおける唯一のｍ番目のビット位置に割り当てられることを意味する。（しかしながら、各々のそしてすべての画素を変更しなければならないとは言えない。）単純化のため、我々は次に、Ｎの独立した信号よりも、１つのマスタコード信号（または“雪状画像”）について述べることができ、このマスタ信号における予め規定された位置が我々のＮビット識別ワードにおける固有ビット位置に対応することを実現する。したがって我々は、この回り道を経て、信号マスタノイズ信号におけるこのある程度簡単な概念を構成する。単なる節約および単純化を越えて、我々のＮビット識別ワードにおける個々のビット位置が、もはや１つの画素／標本の情報輸送容量に対して“十分”でないという考えから元々は得られた、この移動に関する性能的な理由も存在する。

【0195】

この１つのマスタをより明瞭に理解することによって、我々は、この開示の他の部分を新たに見抜くことができ、与えられた用途領域内の更なる詳細を探究することができる。

【0196】

マスタコード概念を使用する大部分の決定論的万能コード

適切な１つの場合は、万能コードに対する部分において項目“２”と呼ばれる、決定論的万能コードの使用をさらに探究することである。この技術の所定のユーザは、この技術の原理の以下の種々の使用を選択することができる。当のユーザを、ホームビデオの大手配給者としてもよいが、明らかに、前記原理は、この技術のすべての他の潜在的ユーザに広がる。図１３は、含まれるステップを図式的に示す。この例において、ユーザを“エイリアンプロダクション”とする。彼等は最初に、彼等の映画“バッドの冒険”のビデオフレームの寸法と同一の空間に広がる画像キャンバスを形成する。このキャンバスにおいて

、彼等は前記映画の名前を印刷し、彼等のロゴおよび社名を配置する。さらに、彼等は、彼等が現在作りだしている大量の複製に対する分配ロットのような特別な情報を下部に有し、示したように、彼等は実際に、示された固有フレーム数を有する。したがって、我々は、オリジナルの映画フレームに付加され、出力配布可能フレームを形成するマスタ雪状画像（マスタコード信号）の形成の初めの基礎を形成する標準画像７００の例を見つける。この画像７００を、白黒またはカラーのいずれとしてもよい。この画像７００を疑似ランダムマスタコード信号に変換する過程は、前記暗号化／スクランブル化ルーチン７０２によって言及され、ここで、オリジナルの画像７００は、なんらかの多数の既知のスクランブル化方法を受ける。番号“２８”の記述は、実際にスクランブル化方法のライブラリとすることができる概念に言及し、この特定の映画、またはこの特定のフレームに使用される個々の方法を変更することができる。その結果、我々の古典的なマスタコード信号または雪状画像となる。一般に、その輝度値は高く、空きチャネルに切り替えたテレビジョン受像機において極めてよく前記雪状画像が見えるが、明らかに、有益な画像７００から得られ、スクランブル化７０２を通じて変換される。（注意：この例の画像の汚れ方は、実際にある程度下手な描写であり、本発明者に利用できる粗末な道具の機能である）。

【0197】

次にこのマスタ雪状画像７０４を、本開示の他の部分において概略を述べた我々のＮビット識別ワードによって変調された信号とし、結果として得られる変調信号を、輝度において、許容しうる知覚されるノイズレベルに低下させ、前記オリジナルフレームに付加し、配布可能フレームを発生する。

【0198】

図１３に示す方法がもたらす種々の利点および特徴が存在する。この変形全体において種々のテーマも存在する。明らかに、１つの利点は、ユーザが、彼等の仕事に押印し、署名するために、より直観的で個人化した方法を使用できることである。暗号化／スクランブル化ルーチン７０２を、高いセキュリティのものとすると共に公開せず、漏洩しないとすると、著作権侵害志望者がロゴ画像７００の知識を有しているとしても、この知識をマスタ雪状画像７０４を追跡することができるようにするために使用することができず、したがって、いわば、本システムを解読することはできない。他方において、簡単な暗号化ルーチンは、本システムを解読するドアを開くことができる。図１３の方法の他の明らかな利点は、他の情報を防御プロセス全体に配置する能力である。正確に言うと、ロゴ画像７００に含まれる情報を、前記最終的な配布可能フレームにおいて直接輸送しない。すなわち、暗号化／スクランブル化ルーチン７０２が、ビット切断エラーを許容する簡単な既知の暗号解読／デスクランブル化方法を有する場合、一般に、配布可能フレームと、Ｎビット識別コードワードと、使用された輝度低下係数と、使用すべき暗号解読ルーチンの数とを有することを基礎として、画像７００を完全に再形成することができる。画像７００の正確な再形成が可能な理由は、前記低下動作それ自体と、相伴うビット切断とのためである。しかしながら、現在の論考に関して、この問題全体は、いくぶんアカデミックである。

【0199】

図１３のテーマにおける変形は、実際にＮビット識別コードをロゴ画像７００に直接配置することである。ある意味において、これは自己参照となる。したがって、我々が、我々の保管するロゴ画像７００を取り出す場合、我々の識別ワードがすでに含まれ、我々は暗号化ルーチン＃２８をこの画像に用い、スケールダウンし、このバージョンを使用し、この開示の技術を使用して疑わしい画像を復号化する。このようにして見つかったＮビットワードは、我々のロゴ画像７００に含まれるものと一致する。

【0200】

暗号化／スクランブル化ルーチン７０２の１つの望ましい特徴を、フレーム番号の１つの数字変化のような小さい変化を入力画像７００に与えた場合、出力スクランブル化マスタ雪状画像７０４において大きな視覚的変化が存在するようになることとしてもよい。さらに、実際のスクランブル化ルーチンは、フレーム番号の関数として変化してもよく、疑

似ランダム化機能において代表的に使用されるある“シード”数が、フレーム番号の関数として変化することができる。したがって、高いレベルのセキュリティを保持するのを助けるすべての変形例の方法が可能である。結局、工学的な最適化の考察が、これらのランダム化方法のいくつかの間の関係と、これらが、非圧縮ビデオストリームを、ＭＰＥＧ圧縮方法論によるように、圧縮ビデオストリームに変換する過程を通じて許容しうる信号強度レベルを保持することにどのように関係するかを研究することを開始するであろう。

【0201】

暗号化過程７０２の他の望ましい特徴は、情報的に効率的である、すなわち、どのようなランダムな入力を与えた場合も、純然たるランダムさを越える残留空間的パターンがわずかであるかまったくない本質的に空間的に一様なノイズ画像を出力できるべきであることである。どのような残留相関パターンも、Ｎビット識別ワードの符号化の非能率化と、他の道具を著作権侵害志望者に公開し、本システムを破壊することとに寄与する。

【0202】

図１３の方法の他の特徴は、復号化システムの部分としての識別できる記号の使用に対するより直観的なアピールであり、これは、法廷の本質的に一般の環境において有利に解釈すべきである。それは、どこかに言及されているコイン投げ固有の単純さ強化する。陪審員または裁判官は、疑わしいコピーを盗まれているとして認識する鍵の１つとしてオーナのロゴをよりよく示すであろう。

【0203】

厳密に言って、ロゴ画像７００はランダム化するためには必要ないことにも言及すべきである。前記ステップを、ロゴ画像７００に直接用いることができる。本発明者には、何が実際的なゴールなのかまったく明らかでない。Ｎ＝１の場合に対するこの概念のささいな拡張は、単純かつ容易に、ロゴ画像７００を単にオリジナル画像に極めて低い輝度レベルにおいて付加する場合である。本発明者は、すべての新規事項においてあるべきこのささいなケースを推定しない。多くの点において、これは、サブリミナル広告の昔からの問題と同様であり、画像に付加された低光レベルパターンは、人間の眼／脳システムに認識可能であり、恐らく、人間の脳において、無意識レベルにおいて動作する。現在の技術のこれらのささいな拡張を指摘することによって、うまくいけば、このような既知の先行技術に関して本願人の新規の原理を識別することをさらに明らかにすることができる。

【0204】

５ビット縮小英数字コードセットおよび他

Ｎビット識別ワードに関する幾つかの用途において、名前、会社、ストレンジワード、メッセージ等を実際に表すことが望ましい。この開示の大部分は、Ｎビット識別ワードを、単に、高い統計上のセキュリティと、インデックス化トラッキングコードと、他のインデックスを基礎とするメッセージ輸送とに使用することに焦点を合わせている。像およびオーディオ内の“不可視署名”の情報輸送容量は、いくらか制限されているが、我々が実際に英数字項目をＮビット識別ワードに“書き込む”場合、我々のＮビットを効率的に使用することが賢明である。

【0205】

これを行うための１つの方法は、英数字メッセージを通過させる減少ビット（例えば、８ビットアスキーより少ない）標準化コードを規定、または、既に存在するものを使用することである。これは、いくつかの用途の一部におけるこの必要性を満たすことを助けることができる。例えば、簡単な英数字コードを、例えば、文字Ｖ、Ｘ、ＱおよびＺを含まないが、数字０ないし９を含む５ビットインデックステーブルにおいて構成することができる。この方法において、１００ビット識別ワードは、２０の英数字記号と共に輸送することができる。他の選択肢は、より頻繁に使用される記号がより短いビット長コードを有し、あまり頻繁に使用されない記号がより長いビット長を有する、テキスト圧縮ルーチンにおいて使用されるもののような可変ビット長コードを使用することである。

【0206】

疑わしい信号におけるＮビット識別ワードを検出し、認識することにおける追加

古典的に言えば、Ｎビット識別信号の検出は、ノイズにおける既知の信号を検出する古い技術によく適合する。この上の文におけるノイズを、極めて広く解釈することができ、下にある署名信号を検出する必要性に関して、画像またはオーディオトラックそれ自体をノイズと考えることができる。このより古い技術に対する多くの参考文献の内の１つは、カッサム、サレーム　エーの本、“非正規ノイズにおける信号検出”スプリンガー－バーラグ，１９８８（よく貯蔵された図書館において一般に利用可能であり、例えば、国会のユー．エス．図書館においてカタログ番号TK5102.５.K357 1988 によって利用できる）である。本発明者の現在の理解の限り、この本における題材を、出願人の埋め込み信号の極性を発見する問題に直接適応できないが、より広い原理を適応できる。

【0207】

特に、カッサムの本の１．２章“仮説検定の基本概念”は、値“１”をある仮説とし、値“０”を他の仮説とすると、バイナリ仮説の基本概念を広げる。この章の最後の段落は、上述した実施形態、すなわち、“０”仮説が“ノイズのみ”の場合に対応し、“１”が観察における信号の存在に対応する場合に関する点にある。しかしながら、真の極性の出願人の使用はこれと同じではなく、ここでは、“０”は“ノイズのみ”よりも反転信号の存在に対応する。本実施形態においても、“ノイズのみ”の場合を実際に無視し、識別過程が、我々のＮビット識別ワードを与えるか、“ゴミ”を与える。

【0208】

埋め込みコード信号の検出における継続し、必然的な工業的改善は、既知の信号検出のこの豊かな分野から、確実に多量に借用するであろう。この分野において普通の良く知られた技術は、いわゆる“適応フィルタ”であり、これは、カッサム本の２章において付随的に説明されている。信号処理における多くの基本的な教科書は、信号検出のこの方法における論考を含んでいる。これは、いくつかの分野において相関検出として既知である。さらに、既知の信号の位相または位置が、しばしばこの技術の用途における場合のように、先天的に既知である場合、適応フィルタを、しばしば、疑わしい画像と我々のＮビット識別ワードにおけるｍ番目のビットプレーンに関係する埋め込み信号との間の簡単なベクトルドット積に減少させることができる。これは、疑わしい画像を取り上げ、その列が予め埋め込まれたＮビット識別ワードに対応するかどうかを決定する目的を有する１および０のシーケンスを発生する、さらに他の簡単な“検出アルゴリズム”を表す。いわば、図３を参照すると、我々は、これらのプロセスステップを進み、オリジナル画像を疑わしい画像から減算することを含み、次のステップは、単に、すべてのＮのランダム独立信号を進むことであり、これらの信号と差信号との単純なベクトルドット積を計算しそのドット積が負の場合、‘０’を割り当て、そのドット積が正の場合、‘１’を割り当てる。この“多くのうちの１つ”のアルゴリズムの慎重な分析は伝統的な適応フィルタとの類似性を示すであろう。

【0209】

極めて低いレベルの埋め込みコード信号を正確に検出する増加した能力を与えることができる、“適応フィルタ”および“相関形式”に対する幾つかの直接的な改善も存在する。これらの改善のいくつかは、前記カッサム本において説明された原理から得られ、他のものは、本発明者によって発生され、本発明者は、他の論文または仕事においてこれらが現れるかについての知識を持たず、進歩した信号検出技術に対する完全な広範囲な調査も行っていない。あるこのような技術は、カッサム本の７９ページの図３．５によって例示されるものがひょっとすると最適であり、検出のための一般的なドット積アルゴリズムアプローチに用いることができる種々の局所的最適化重み付け係数のいくらかのプロットが存在する。すなわち、単純なドット積を計算するよりも、全体のドット積における各々の要素的乗算を、差信号それ自体に、すなわち、低レベルの既知の信号が探索されている中の信号についての既知の先天的統計情報を基礎として重み付けすることができる。これらの話題にまだ精通していない興味を持った読み手には、カッサムの３章を読み、より完全な理解を得ることを薦める。

【0210】

カッサムの本において明白に存在するように見えず、本発明者によって基礎的に開発されたある原理は、全体として、疑わしい信号の統計的特性の大きさに対する、捜している既知の信号の統計的特性の大きさの利用を含む。特に、問題の場合は、我々が捜している埋め込まれた信号が、差信号において存在するノイズおよび改ざんよりもかなり低いレベルである場合であるように思われる。図１４は、このアプローチに続く推論に対するステージの設定を試みる。上部の図７２０は、代表的な“問題の”差信号、すなわち、その中に存在するかもしれず、存在しないかもしれない埋め込まれた信号よりもかなり高い全体的なエネルギを有する差信号のヒストグラムにおける差における一般的な様子を含む。“平均を除去した”という言葉は、単に、差信号および埋め込まれた信号の双方の平均が、規格化ドット積を行う前の一般的な演算によって除去されていることを意味する。次に、下部の図７２２は、これら２つの信号の導関数、または画像の場合においてスケーラ勾配の一般的な同様のヒストグラムプロットを有する。純粋な検査から、導関数変換領域における簡単なしきい値化演算と、その後の信号領域への逆変換とは、いくつか前のパラグラフのドット積“識別アルゴリズム”におけるある程度の先天的なバイアスを取り除くことに向かう長い道を行くことになる。ここで、しきい値化は、差信号導関数値の絶対値があるしきい値を越える場合、そのしきい値を単に置き換えるというアイデアのことを呼ぶ。このしきい値を、埋め込まれた信号のヒストグラムを最大に含むように選択することができる。

【0211】

ドット積アルゴリズムにおけるバイアス効果のいくつかを“軽減する”ことにおける重要でない援助とすることができる他の演算は、差信号における低次周波数の除去であり、すなわち、差信号をハイパスフィルタに通すことであり、ここで、ハイパスフィルタに関するカットオフ周波数を、元の（またはＤＣ）周波数に比較的近くする。

【0212】

圧縮され、伸張された信号における埋め込み信号を認識するか、非一様エラー源を形成するある既知のプロセスを受けたなんらかの信号内の埋め込み信号を認識する特別な考察

基本概念に関する長いタイトル。画像／ビデオ圧縮のＪＰＥＧ／ＭＰＥＧフォーマットによる画像の圧縮および伸張のような、いくつかの信号処理動作は、ある相関および構造を有するある一定の変換領域においてエラーを形成する。例としてＪＰＥＧを使用すると、所定の画像をいくらか高い圧縮比で圧縮し、伸張し、結果としての画像をフーリエ変換し、オリジナルの非圧縮画像のフーリエ変換と比較すると、一定のパターンが明白に可視になる。このパターン化は、相関エラー、すなわち、ある程度量化でき、予測できるエラーのしるしである。この相関エラーのより酷い特性の予測を、ＪＰＥＧ圧縮か、これらの見てすぐそれと分かるエラー署名を残す他の動作かを受けたかもしれないある疑わしい画像内の埋め込みコード信号を認識するこれまでに論じた方法において有利に使用することができる。基本的なアイデアは、既知のより高いレベルのエラーが存在する領域において、前記認識方法の値は、既知のより低いレベルの相関エラーを有する領域に対して小さくなることである。しばしば、エラーの予測されるレベルを量化し、この量化を再変換された信号値を適切に重み付けすることに使用することができる。再び例としてＪＰＥＧ圧縮を使用すると、疑わしい信号をフーリエ変換することができ、フーリエ空間表現が、見てそれと分かる箱格子パターンを明らかに示すことができる。次にフーリエ空間信号を、格子点付近で“空間フィルタ処理”することができ、次にこのフィルタ処理化表現を、その通常の時間または空間領域に変換し戻し、次に本開示において与えた認識方法を行うことができる。同様に、非一様エラー源を形成するなんらかの信号処理方法を、これらのエラー源が非一様となる領域に変換することができ、これらのエラー源の高い点における値を減少させることができ、このように“フィルタ処理された”信号を、標準的な認識のための時間／空間領域に変換し戻すことができる。しばしば、この全体のプロセスは、適切なフィルタ処理プロファイルを“設計”するために、代表的な相関エラーの動作を“特徴化”する長く困難なステップを含むであろう。

【0213】

“署名コード”および“不可視署名”

簡単に、かつ明瞭にするために、“署名”、“不可視署名”および“署名コード”という言葉を、科学技術の一般的な技術を示し、しばしば、特に本開示において前に規定した複合埋め込みコード信号を示すために使用し、使用し続ける。

【0214】

動画への署名コード埋め込みにおける更なる詳細

静止画を圧縮するＪＰＥＧ標準と、動画を圧縮するＭＰＥＧ標準との間に差があるため、不可視署名を静止画に配置することと、署名を動画に配置することとの間にも差がある。ＪＰＥＧ／ＭＰＥＧ差によるように、異なる基礎の問題ではなく、動画によって、パラメータとして時間を含むことによって、工業的最適化の新たな次元が開くことである。ＭＰＥＧに関係するどの教科書も、どのようにＭＰＥＧが（一般に）単にＪＰＥＧをフレームずつを基礎として用いていないかについての部分を必ず含むであろう。この技術の原理の用途と同じく、一般的に言って、動画シーケンスへの不可視署名の配置は、単に別々に不可視署名をフレーム毎に配置することではない。動画知覚の精神物理学にいくらか関係する種々の時間を基礎とする理由が作用し、他は、単純な費用工学的理由によるものである。

【0215】

ある実施形態は、実際に、ＭＰＥＧ圧縮標準を解決法の１つとして使用する。すでに発明されているか、まだ発明されていない他の動画圧縮方法を、等しく良好に使用することができる。本例は、図１３に示し、本開示において論考したマスタ雪状画像の発生のために、スクランブル化ロゴ画像アプローチも使用する。

【0216】

“圧縮マスタ雪状画像”を、図１５に示すように別個にレンダリングする。“レンダリング”は、ビデオ、映画およびアニメーション制作において一般に既知の技術を示し、これによって、画像または画像のシーケンスを、コンピュータ命令のような構成的技術か、手によるアニメーションセルの描画によって形成する。したがって、本例における署名映画を“レンダリングする”ことは、本質的に、ディジタルファイルとしてコンピュータ形成しようとすることか、それを形成するあるカスタムディジタル電子回路網を設計することである。

【0217】

図１５において概要を示した手順の全体的なゴールは、不可視署名をオリジナルの映画７６２に、前記署名が並べて観る、７６８によって記憶される前記映画の商業的価値を落とさず、前記署名がＭＰＥＧ圧縮および伸張プロセスを経ても最適に残存するように用いることである。上記で示したように、特にＭＰＥＧプロセスの使用が、圧縮の一般的なプロセスの一例である。また、ここで与えた例が、工業的変形に関して一定の能力を有することに注意すべきである。特に、動画圧縮の技術において実行されているこれらは、我々が２つのビデオストリームＡおよびＢで開始し、ＡおよびＢを別々に圧縮し、これらの結果を結合する場合、結果として生じるビデオストリームＣは、ビデオストリームＡおよびＢを予め結合し、この結果を圧縮した場合とは一般に同じにはならないことが分かる。したがって、一般に、例えば、

ＭＰＥＧ（Ａ）＋ＭＰＥＧ（Ｂ）≠ＭＰＥＧ（Ａ＋Ｂ）

となる。これは、本開示におけるこの点においていくぶん抽象的な概念を導入し、図１５を論考するためにより明らかになるであろう。しかしながら一般的なアイデアは、圧縮手順の“不可視”署名の通過を最適化するのに使用できる種々の代数学が存在することである。明らかに、図１５に示すのと同じ原理は画像に依然として効果があり、ＪＰＥＧまたは他のものが依然として画像圧縮の標準である。

【0218】

ここで図１５の詳細に戻り、映画またはビデオのすべてのＺフレームを通じて単純にステップすることから始める。一秒あたり３０フレームで上映される２時間映画に関して、Ｚは、（３０＊２＊６０＊６０）すなわち２１６０００となる。７００、７０２および７

０４の内部ループは、単に図１３のステップの模倣である。ロゴフレームを、フレームのステップ中任意に変更することができる。ボックス７０４から放射する２つの矢印は、ループ７５０の継続と、出力フレームのレンダリングマスタ雪状画像７５２への配置とを表す。

【0219】

この点において短いが可能的に適切な余談をすると、マルコフ処理の概念の使用は、図１５の工業的実現化の最適化に関する議論をいくらか明瞭にする。簡単に、マルコフ処理は、イベントのシーケンスが起こり、一般的に、このシーケンスにおける１ステップと次のステップとの間に記憶が存在しない処理である。図１５の状況および画像のシーケンスにおいて、画像のマルコフ的シーケンスは、所定のフレームと次のフレームとの間に明らかなまたは多少の相関関係がないシーケンスである。これまでに制作されたすべての映画の組を取り、同時に１つのフレームをステップし、出力映画に挿入すべきランダムな映画からランダムなフレームを選択し、一分すなわち１８００のこれらのフレームを通じてステップすると仮定する。結果として生じる“映画”を、マルコフ映画の良い例とする。この論考の１つの点は、ロゴフレームをどのようにレンダリングするかに応じて、暗号化／スクランブル化ステップ７０２をどのように行うかに応じて、マスタ雪状映画７５２が、ある一般的な量化できる程度のマルコフ的特徴を示すであろうことである。この点の要点は、圧縮手順それ自体が、このマルコフ的特徴の程度によって影響され、したがって図１５の過程の設計において考慮する必要があることである。同様に、かつ単に一般的に、完全にマルコフ的な映画を高輝度マスタ雪状映画７５２において形成したとしても、ＭＰＥＧボックス７５４として表されるその映画の圧縮および伸張処理は、７５２のマルコフ的特性の幾らかを減衰させ、少なくとも最低限に非マルコフ的な圧縮マスタ雪状映画７５６を形成する。この点を、本開示が１つのＮビット識別ワードを見つけるためにビデオストリームの多数のフレームを使用するアイデアを論じるときに使用し、すなわち、同じＮビット識別ワードを映画のいくつかのフレームに埋め込むことができ、これらの多数のフレームから得られた情報を使用し、その１つのＮビット識別ワードを見つけることは、全く合理的である。したがって、７５６の非マルコフ的特性は、前記不可視署名の読み出しおよび認識にいくつかの手段を加える。

【0220】

最終的に使用されるマスタ雪状映画７５６を前調節する目的により、ここで、レンダリングされた高輝度マスタ雪状映画７５２をＭＰＥＧ圧縮および伸張手順７５４を経て送る。ＭＰＥＧ圧縮は一般的に分配的でないと認められる上述した注意により、ステップ７５４のアイデアは、初めにレンダリングした雪状映画７５２を２つの成分、７５６である圧縮処理７５４を免れる成分と、免れない成分とに大雑把に分離し、差演算７５８を使用して大雑把に推定し、“安っぽいマスタ雪状映画”７６０を発生することである。故意に散漫な言葉“安っぽい”を使用した理由は、恐らく共通の圧縮処理を免れないにも係わらず、圧縮を決して受けない用途または状況に対して“安っぽい”特別の署名信号エネルギを発生できることを知ることにより、この署名信号を同様に配布可能映画に後に付加することができるためである。（したがって、図１５において少なくとも示す。）図１５に戻り、我々は、圧縮処理を不変のまま残存する高い可能性を有することを知っている署名における荒い切断を行い、この“圧縮マスタ雪状映画”７５６を使用し、縮小した７６５であるこの手順を通り、オリジナル映画と比較（７６８）し、セットアップされているどのような商業的実行可能規準（すなわち、許容しうる知覚されるノイズレベル）にも適合することを保証する。並べて観るステップ７６８から縮小ステップ７６４に戻る矢印は、図２の“視覚的実験．．”と、図６のゲイン制御２２６とに直接対応する。画像および音響理論における当業者は、図１５の全体を、前記可視署名信号の、これらが完全に感知しうる圧縮さえもより耐えられるような前調節を試みることによって要約できることを認識できる。上述した項目を同様に反復するため、このアイデアを、画像、画像シーケンスまたはオーディオトラックに受けさせてもよいなんらかのこのような前識別可能処理に等しく用いる。これは、明らかに、静止画へのＪＰＥＧ処理を含む。

【0221】
リアルタイムエンコーダ回路網の追加要素
一般に、ボックス７５０から圧縮マスタ雪状映画の形成７５６を経て続く図１５に示す方法ステップを、ある変更によって、ハードウェアにおいて実現することができることに注意されたい。特に、図６におけるアナログノイズ源２０６全体を、このようなハードウェア回路によって置き換えることができる。同様に、図１３において示すステップおよび関係する手順を、ハードウェアにおいて実現することができ、アナログノイズ源２０６を置き換えることができる。
【0222】
２フレーム以上を基礎とする認識：非マルコフ的署名
画像のマルコフおよび非マルコフシーケンスにおける余談において示したように、埋め込み不可視署名信号を非マルコフ的性質である、すなわち、あるフレームのマスタ雪状画像と次のフレームのそれとの間にある相関関係が存在し、さらに、１つのＮビット識別ワードをフレームの範囲に渡って使用し、フレームのシーケンスに関係するＮビット識別ワードのシーケンスが非マルコフ的特徴である状況において、１つのＮビット識別ワードを認識するため、映画またはビデオのいくつかのフレームからのデータを使用できる点を、再び指摘する。このすべては、不可視署名を認識する処理は、動画シーケンスの多数のフレームに変換するこの場合において、利用できる情報だけを使用すべきであるということを言う想像的な方法である。
【0223】
ヘッダ変形例
ディジタル画像またはオーディオファイルにおける“ヘッダ”の概念は、当該技術分野において十分に確立された理論である。図１６の上部は、ヘッダの概念における単純化した外観を有し、ここで、データファイルは、一般に、全体としてのファイルについての情報の包括的な組から始まり、しばしば、著作権者がいるなら、データの著者または著作権保持者である人についての情報を含む。このヘッダ８００に、代表的に、オーディオストリーム、ディジタル画像、ビデオストリームまたはこれらの項目の圧縮したもののようなデータそれ自体８０２が続く。これは、工業においてよく知られており、共通である。
【0224】
この技術の原理を情報保全のサービスに用いることができる１つの方法を、図１６の下部に一般的に示す。一般的に、Ｎビット識別ワードを、画像（図示するような）またはオーディオデータストリーム全体の本質的に“壁紙”の所定の簡単なメッセージに使用することができる。これを、この節のタイトルにおける“ヘッダ変形例”と呼ぶ。ここでの考えは、あまり洗練されていない著作権侵害志望者および悪用者がヘッダ情報の情報内容を変更することができ、したがってこのテクノロジーのより安全な技術をヘッダ情報の真実性における検査として使用できることである。ヘッダにおける“ジョーの画像”のようなコードメッセージを与えた場合、ユーザが得る画像は、ヘッダの変更が行われないことの、あるより高い程度の信頼性を有することができる。
【0225】
同様に、前記ヘッダは、実際にＮビット識別ワードを輸送することができるため、所定のデータセットをこのテクノロジーの方法によって符号化したことを強調することができ、識別コードを前記ヘッダに正確に組み込むことができる。当然、このデータファイルフォーマットは、このテクノロジーの原理が現在用いられていないことから、まだ形成されていない。
【0226】
“ボディア”：ヘッダの大きい変換に対する能力
本願人のテクノロジーの以下の態様のすべての可能な用途が完全に開発されていないとしても、いつか重要になるかもしれない設計変更として与える。この節のタイトルは、この可能性を説明するために使用する馬鹿な言い回し、“ボディア（ＢＯＤＩＥＲ）”を含む。

【0227】
前節では、Ｎビット識別ワードが、ディジタルファイルのヘッダに含まれた情報をどのように“識別するかについての概略を述べたが、これらの方法が、ヘッダの概念を完全に置き換えることができ、ヘッダに慣例的に格納された情報を、ディジタル信号および経験的データそれ自体に配置することができる予想も存在する。
【0228】
これを、単に例として、別の完全に経験的なデータストリームにおける９６ビット（１２バイト）リーダストリングにおける標準化と同じ位簡単にすることができる。このリーダストリングは、リーダストリングを含まない全体のデータファイルの、要素的データユニットにおける数字長と、１つのデータ要素の深さのビット数（例えば、グレイレベルの数またはオーディオ信号の離散的信号レベルの数）とを、明瞭かつ単純に含む。これらから、本明細書に記載の万能コードを使用し、経験的データ内に直接書き込まれたＮビット識別ワードを読み出す。前記経験的データの長さは、完全なＮビットを含むのに十分な長さとする必要がある。Ｎビットワードは、そうでなければ慣例的なヘッダに含まれるものを能率的に伝送する。
【0229】
図１７は、このようなデータフォーマットを示し、これを“万能経験的データフォーマット”と呼ぶ。リーダストリング８２０は、６４ビットストリング長８２２と、３２ビットデータワードサイズ８２４とから成る。次にすぐデータストリーム８２６が続き、ヘッダに慣例的に含まれるが、ここではデータストリームには直接含まれない情報を、付加した点線８２８として表す。この付加した情報に使用した他の言葉は、図１７にも示す“影チャネル”である。
【0230】
リーダストリングに含めることが必要な他の要素は、データファイルの全体が変更されていないことを識別できるある種の複合チェックサムビットである。
【0231】
配布された万能コードシステムにおける他：動的コード
万能コードのテーマにおける１つの興味深い変形は、万能コードそれ自体の動作を変更する命令を実際に含むＮビット識別ワードの可能性である。多くの例のうちの１つは、データ送信が開始し、そこで、オーディオデータの所定のブロックが完全に伝送され、Ｎビット識別ワードを読み出し、５００の組から万能コード＃１４５が使用するデータの第１ブロックと、このように見つかったＮビット識別ワードの部分が、データの次のブロックを万能コードセット＃１４５よりも＃４１１を使用して分析すべきである命令であることとを知る。一般的に、このテクノロジーを、実際の復号化命令自体をオンザフライで変更する方法として使
用することができる。さらに一般的に、“動的コード”を使用するこの可能性を、データ識別手順の洗練レベルを大きく上昇させ、ハッカーおよび著作権侵害志望者によってあまり洗練されていない妨害を受ける傾向があるシステムの経済的生存能力を増加させるべきである。本発明者は、復号化／暗号解読命令の動的変化の概念自体が新規であるとは信じていないが、経験的データの“影チャネル”におけるこれらの命令の実行は、本発明者の理解する限り、新規であると思われる。（影チャネルは、このテクノロジーのよりステガノグラフ的な適切な要素をカプセル化する他の専門的言い回しとして規定されている）。
【0232】
動的コードのテーマにおける変形は、その時どのコードを使用するかについての先天的に割り当てられた知識を有するシステムにおける万能コードの使用である。この可能性をまとめる１つの方法は、“デイリーパスワード”のアイデアである。この例におけるパスワードは、どの万能コードの組が現在動作するかの知識を表し、これらは、用途特定環境のある組に応じて変化する。恐らく、多くの用途が、万能コードをまだ一度も使用さていないものに対して連続的に更新し、これは、デイリーパスワードの慣例的な概念によくある場合である。現在伝送されているＮビット情報ワードの部分を、例えば、次の日のパス

ワードの経過とすることができる。例え、時間がパスワードの変更の最も普通のトリガイベントであるとしても、同様にイベントを基礎とするトリガがあってもよい。

【0233】

対称パターンおよびノイズパターン：強固な万能符号化システムのために

識別パターンの画像への配置は、確かに新しくない。画像のコーナにスタンプされたロゴ、真の署名や著作権の丸Ｃ記号のような微細なパターン、および、透かしが、所有権を表すため、または、創造的題材の不正な使用を防ごうとするためにパターンを画像に配置することの例である。

【0234】

新規であると思われるものは、独立した“キャリヤ”パターンを配置するアプローチであり、これらのパターンは、それら自体を、ある情報と共に、前記情報の伝送および識別の目的のために画像およびオーディオ内に直接変調することができるものである。本発明者に現在既知のステガノグラフィ的解決法は、すべてこの情報を経験的データに“直接”配置する（できる限り最初に暗号化し、次に直接）が、本開示の方法は、これらの（非常にしばしば）同一空間キャリヤ信号の形成と、これらのキャリヤ信号の適切な情報との変調と、経験的データへの直接の適用とを仮定している。

【0235】

これらの概念の拡張において、さらに万能コードシステムの用途の舞台に一歩進み、ここでは、送信サイトは使用される特定の万能コード化計画によって経験的データを送信し、受信サイトは前記万能コード化計画を使用して前記経験的データを分析し、オーディオとは相違して画像または動画の伝送用に設計されたこのようなシステムの工業的理由において近い様子をとることが有利である。より明瞭に言うと、図９とこれに伴うオーディオ用途における万能コードについての論考に含まれるような特定の実現化の分析と同じタイプの分析を、画像（または２次元信号）にも同様に行うべきである。この節は、万能コードの特定の実現化のこのような分析および概略であり、このような方法が明らかにすべき種々のハードルを予測することを試みる。

【0236】

画像および動画用万能コード化システムの一実現化の統合するテーマは、“対称”である。これを進めるアイデアは、より簡単に、あまり洗練されていない著作権侵害者が、なにか与えられた万能コード化システムを迂回する意味として、画像循環の使用に対する予防とすることはできない。先導する原理は、万能コード化システムを、従属する画像がどの回転方向にあっても容易に読み取れるべきであるということである。これらの問題は、光学文字認識および物体認識の分野において共通であり、これらの分野を、このテクノロジーの工業的実現化の促進における他の方法および手段に関して参照すべきである。通常、直接的な例は順序である。

【0237】

ディジタルビデオおよびインターネットカンパニーＸＹＺは、入力ビデオを二重検査し、ビデオそれ自体の個々のフレームである視覚的データが、このテクノロジーを使用するＸＹＺのそれ自体の比較的高い安全性の内部署名コードを含む、非対称万能コード化を頼るその製品の配達システムを開発している。これは、ヘッダ情報が照合されると共にフレーム内万能コードが見つからなければどのような題材も通さない彼等のインターネット関門を含む、多くの配達状況において良好に働く。しかしながら、これらの商業的ネットワークの他の部分は、インターネットチャネルにおいて世界のルーチン監視を行い、彼等の所有の創造的財産の許可されない伝達を見つける。彼等は、使用される暗号化手順を制御し、したがって、ヘッダを含む創造的財産を暗号解読し、簡単な検査をすることは、彼等にとって問題ではない。ＸＹＺのネットワークにおいて題材を売買したい著作権侵害者グループは、ＸＹＺのヘッダ情報システムにおけるセキュリティ特徴をどのように変更するかを決定しており、さらに、１０または２０程度の画像を単純に回転させ、ＸＹＺネットワークに送信することによって　ネットワークは、コードを認識せず、したがって、彼等の題材の不正使用にフラグを立てず、著作権侵害者が回転した題材の受取人は、それを簡

単に回転しない。

【0238】

この最後の例を論理的な分類を経て要約すると、非対称万能コードは、“コードの発見を基礎とする許可された動作の可能化”に対して許容しうるものであるが、“コードの存在に関するランダムな監視（取締り）”の場合において多少容易にバイパスされる恐れがある。〔非対称万能コードは、不正使用の９０％を極めて良好に捕らえることができる、すなわち、不正使用者の９０％が回転の単純なバイパスをするに悩まないことを主張する〕この後者の範疇にアドレスするために、疑似回転対称万能コードの使用を必要とする。回転問題を四角にする長年からの“疑似”装置は、この瞬時の変換において、完全に増加する回転対象オブジェクトを画素の正方格子において表すことはできない。さらに、基本的考察を、万能コードのスケール／大きさ変化に対して行う必要がある。監視プロセスを、監視される視覚的題材が“知覚”領域にある場合、すなわち、暗号化されておらず、スクランブル化されておらず、人間の見る人に対して与えられる（または与えられるであろう）形態にある場合、行う必要があることが理解される。著作権侵害志望者は、他の簡単なスクランブル化および非スクランブル化技術を使用することができ、道具を、これらの漏洩するスクランブル化信号を監視するために開発することができる。すなわち、著作権侵害志望者は、視覚的題材を知覚領域外に変換し、監視点によって通過し、前記題材を知覚領域に逆変換することを調査し、万能コードの監視と異なる道具が、このようなシナリオにおいて使用することが必要である。したがってここで考察した監視を、監視を知覚領域において行えるような用途に対して用い、このような場合、見る設備を実際に送る。

【0239】

“リング”は、唯一の完全な回転対称２次元物体である。“ディスク”を、それらの半径軸に沿って幅を有する同心で完全に接触しているリングの単純な有限の組と見なすことができる。したがって、“リング”を、画像に対するより堅牢な万能コード標準がそこから見つかる開始点とする必要がある。リングは、スケール／倍率変更の問題にも良好に適応し、リングの半径がそのトラックを保持し、顧慮する１つのパラメータである。リングの他の特性は、異なったスケール変化が画像における異なった空間軸に対して起こり、リングが楕円になる場合でも、どのような自動化監視システムも求めている滑らかで疑似対称特性の多くが一般的に維持されることである。同様に、どのような画像の感知しうる幾何学的歪みも、リングを明らかに歪ませるが、これらは依然として全部の対称特性を保持することができる。うまくいけば、単純に画像を“観る”ようなより平凡な方法で、これらの関係において、特に、このような長さが万能コード化システムをバイパスする場合、試みられた不正な著作権侵害を検出できるであろう。

【0240】

リング対ノット

リングを、その基礎に応じて完全循環的堅牢万能コード化システムを構築できる唯一の理想的な対称パターンとして発見したことにより、我々は、この基本的なパターンを、情報を輸送でき、コンピュータまたは他の手段によって読み出すことができ、簡単な変換および改ざんを生き抜くことができ、簡単なコスト増加項目としての破壊の経済性を保持するために、（万能コードにおける節で説明したように、恐らく壊すことができなくない）高いレベルのセキュリティに合理的に上昇させることができる何か機能的な何かに変えなければならない。

【0241】

“リングを基礎とする”万能コードの一例は、本発明者が、後に洗練され、レオナルド　ダ　ヴィンチの仕事（例えば、モナリザまたは彼のノット図案）において高められた、織られたケルトのノットパターンにしたがって、“ノットパターン”または単に“ノット”と呼ぶものである。いくつかの噂は、ノットのこれらの絵は、実際にステガノグラフィ的であり、すなわち、メッセージおよび署名、すなわち、より固有のものすべてを伝達することをもたらしている。図１８および１９は、これらのノットパターンの基本的な特性の幾つかを調査する。

【0242】
ノットパターンの２つの簡単な例を、超放射ノット８５０および放射ノット８５２によって示す。これらの形式の名前は、拡がったリングの中心の対称点と、構成するリングがこの点と交差するか、完全にその外側か、サブ放射ノットの場合、前記中心点構成する円の内側であるかどうかとを基礎とする。８５０および８５２の例は、明らかに、８個のリングまたは円の対照的配置を示す。“リング”を、上述したように、この言葉は、リングの放射軸に沿ったリングの幅を明白に認めるという点で、より固有の言葉とする。ノットパターン８５０および８５２における個々のリングは、我々のＮビット識別ワードにおけるビットプレーンに関係する信号のためのキャリヤ信号となるであろう。したがって、ノットパターン８５０および８５２の各々を、８ビット情報キャリヤとする。特に、ノットパターン８５０および８５２を、黒い背景における明るいリングとすると、独立したソース画像への明るいリングの“加算”が“１”を表すことができ、独立したソース画像からの明るいリングの“減算”が“０”を表すことができる。この簡単な符号化計画の適用を、図１９とそのノットパターンのモザイクにおけるように、何度も反復することができ、この符号化（変調化）ノットモザイクのスケールダウンバージョンを、オリジナル画像に直接かつ同一の時間に渡り追加する最終ステップと、この万能対称コード化方法を経て符号化された配布可能画像とする結果とを伴う。どのリングが我々のＮビット識別ワードにおける最下位ビットであり、どれが最上位ビットであるかを、復号化システムと通信することが残っている。１つのこのような方法は、（個々のリングの）半径値のスケールをＬＳＢからＭＳＢまでわずかに増加させることである。他の方法は、単に、ＭＳＢを他のものより１０％大きい半径とし、残りのビットが一致しない順序としてカウンタクロック幅を予め割り当てることである。さらに他の方法は、ある簡単なハッシュマークをただ１つの円の内側に置くことである。すなわち、リングのビット順序をこれらのノットパターンにおいて符号化することができる種々の方法が存在する。

【0243】
最初にこれらのノットパターンの単なる存在に対して検査し、第２にＮビット識別ワードの読み取る手順は、以下のようなものである。疑わしい画像を、最初に、極めて普通の２Ｄ　ＦＦＴコンピュータ手順を経てフーリエ変換する。我々は、ノットパターンの正確なスケールを知らないとし、すなわち、我々は、画素の単位におけるノットパターンの要素的リングの直径を知らず、我々は、ノットパターンの正確な回転状態を知らず、我々は単に、警告する波紋パターンに関するオリジナル画像のフーリエ変換の結果としての振幅（ソース画像の空間周波数プロファイルの頂点における同心低振幅正弦リング）を（基本的な自動化パターン認識方法によって）検査するとする。リングの間隔と共にこれらのリングの周期性は、万能ノットパターンが存在すると思われるかまたは思われないかと、画素におけるこれらのスケールとを我々に知らせるであろう。古典的な小さい信号検出方法をこの目的に、この開示の他の検出方法を用いることができるように用いることができる。次に普通の空間フィルタ処理をフーリエ変換した疑わしい画像に用いることができ、ここで、使用すべき空間フィルタは、同心円の頂点におけるすべての空間周波数を通過させ、他のすべの空間周波数をブロックする。結果として得られるフィルタ処理化画像を、空間周波数領域から画像空間領域にフーリエ変換し、ほとんど視覚的検査によって、明るいリングの反転または非反転を、ＭＳＢまたはＬＳＢリングの識別と、Ｎ（この場合において８）ビット識別コードワードと共に見つけることができる。明らかに、パターン認識手順が、この復号化ステップを同様に行うことができる。

【0244】
前述の論考およびそれが説明する方法は、ある実際的な欠点と、ここで論考し改善する欠点とを有する。基本的な方法を、含まれる基本的な原理を伝えるために、素朴な様式において与える。

【0245】
ノットパターンを使用する上述した万能コード化システムのいくつかの実際的な困難を列挙しよう。一例として、（１）リングパターンは、全部の画像空間を“覆うこと”にお

いて、そして、画像範囲の情報輸送容量のすべての使用において、いくぶん非能率的である。第２に、（２）リングパターン自体が、これらを例えば８ビット白黒画像に対する単純な付加方法において用いた場合に、より可視である必要がある。次に、（３）図１８の“８”リング８５０および８５２はむしろ少ない数であり、さらに、認識方法が対応する必要がある図に用いることができる２２．５度の回転が存在する。次に、（４）リングの完全な重なりが、加算され減算された輝度が完全に感知できるようになってしまう、高く凝縮された領域が発生する。次に、（５）復号化において使用した２Ｄ　ＦＦＴルーチンは、言及されているパターン認識方法のいくつかと同様に、計算上扱いにくいことが有名である。最後に、（６）これにもかかわらず、ここまで説明した万能コード化の形態は、最高のセキュリティ通信システムの古典的なセンスにおける超高いセキュリティを有することを主張せず、それにもかかわらず、ハードウェアおよびソフトウェアにおいて実現するのに費用が掛からず、同時に、著作権侵害志望者がシステムの裏をかこうと試みる費用が増加し、これらの著作権侵害者に必要な洗練度レベルが上昇という、ある程度のセキュリティ特徴を、著作権侵害志望者が、たくらみが容易に証明され、うまくいけば（これらのノットパターンコードの創造的所有権を奪う手段の形成および配布のような）激しい犯罪の責任および刑罰を受けさせるシステムの裏をかく彼等の方法から進まなければならない点に対して、有利に付加する。

【0246】

これらの項目のすべてを取り上げることができ、前記テクノロジーの原理のどのような工業的実現化においても、改良しつづけるべきである。本開示は、以下の実施形態の参照と共にこれらの項目を取り上げる。

【0247】

項目番号３から始め、図１８に示す８つのリングのみが存在することを、単にリングの数の増加によって補う。所定の用途が使用するであろうリングの数は、明らかにその用途の関数である。トレードオフは、使用するリングの数を制限することを主張する側において、少ないリングが存在する場合、最終的にリング当たり（可視度あたり）より多くの信号エネルギが存在し、自動化認識方法によるその識別が容易になるように、リングをあまり集めず、一般的に、これらはあまり集まっていないことから、全部のノットパターンを、より小さい全体の画素範囲、例えば、１００画素直径領域よりも３０画素直径領域を使用して含めることができるといったことを含むが、これらに限定されない。リングの数を増加させる理由は、アスキー情報、シリアル番号、アクセスコード、使用可能コードおよび履歴情報、等のようなより多くの情報を伝達する欲求を含み、より多くのコードを有することの他の鍵となる利点は、ノットパターンのそれ自体への回転が減少し、それによって、前記認識方法がより小さい範囲の回転角を扱えるようにすることである（例えば、６４のリングは、３度以下の最大回転変移を有する、すなわち、そのオリジナルパターンに対して最大に異なり、５．５度程度の回転は、ノットパターンをその初期アラインメントにならせ、ＭＳＢ／ＬＳＢおよびビットプレーン順序を識別する必要性は、この例において同様によりよく理解できる）。大部分の実際的な用途は、Ｎビット識別コードワードにおけるビット数の選択に対するＮ＝１６ないしＮ＝１２８に対応する１６ないし１２８リングを選択する。この選択の範囲は、８５０または８５２のような要素的ノットパターンに割り当てると、すべての半径と画素において幾分相関する。

【0248】

画像におけるリングパターンの集中と、他のことにおけるリングパターンの欠如（極めて類似しているが、項目１の非能率な覆うこととは異なる）である実際的な困難の項目番号４を取り上げると、以下の改善を用いることができる。図１８は、“ノット”（リングのパターンとの対比として）の鍵となる特徴の一例を示し、パターンがおそらく交差する場合、仮想の第３次元を仮定し、それにより、ノットのある場所が、ある予め決められた方法において、他の場所よりも優先する（項目８５４参照）。像の見地から、ノットパターンにおける所定の交差点の輝度または暗さを、２つ以上の場所が重なる領域において１つの場所のみに“割り当てる”。このアイデアを、この割り当てについてのルールをある

回転対称方法においてどのように行うかに拡張する（８６４）。例えば、ルールを、時計方向に進むことにより、ループに入ってくるひもが、出ていくひもの後ろになることにする。明らかに、これらのルールに用いることができる多数の変形例が存在し、その多くは、選択したノットパターンのジオメトリに決定的に依存する。含まれる他の問題は、恐らく、有限の幅と、さらに、ひもの方向に対して垂直の軸に沿った幅の輝度プロファイルとが、ノットパターンの下にある所定の画素への輝度割り当てのルールにおいてそれぞれ役割を演じることであろう。

【0249】

上述した名目上のノットパターンシステムに対する主要な改善は、実際的な困難、（１）非能率的に覆うこと、（２）リングの望ましくない可視度、および（６）高いレベルのセキュリティの必要性を直接取り上げる。この改善は、直前の節において論考した項目（４）重なり問題も間接的に取り上げる。この主要な改善は、以下の通りである。符号化ノットパターンのモザイクをオリジナル画像に付加し、配布可能画像を発生するステップの前に、符号化ノットパターンのモザイク８６６を、標準化され、（一般的に滑らかに）ランダムな位相のみの空間フィルタによって、（普通の２Ｄ　ＦＦＴ技術を使用して）空間的にフィルタ処理する。この位相のみのフィルタが、空間周波数領域においてそれ自体完全に回転対称であり、すなわち、そのフィルタ処理作用が完全に回転対称であることに注意することは、極めて重要である。個々の輝度リングにおけるこの位相のみのフィルタの作用は、同心リングの滑らかに変化するパターンに変換し、このパターンは、石を落とした後のいくつかの場合における水上のパターンとまったく異なってはおらず、波パターンが、この位相のみのフィルタの場合において、石波パターンの一様な周期性よりも、いくぶんランダムである。図２０は、これらの位相のみフィルタ処理化リングパターンの粗い（すなわち、非グレイスケールの）表現を与える。図２０の上部の図は、これらの位相のみフィルタ処理化リングパターンの１つの代表的な輝度輪郭／プロファイルの断面図８７４である。個々のリングの中心８７２を、これらのフィルタ処理化パターンの１つの２次元輝度分布を完全に記述するために、前記輝度プロファイルをその回りで回転させる点とする。フィルタ処理化リングの特性を伝えるさらに他の粗い試みを、フィルタ処理化リングの大雑把なグレイスケール画像８７６として表す。この位相のみフィルタ処理化リング８７６を、ランダム波状パターンと呼ぶことができる。

【0250】

図２０に示さないことは、図１８のノットパターンまたは図１９のノットパターンのモザイクにおける位相のみフィルタ処理の合成作用である。ノットパターン８５０または８５２における各々のリングは、８７６の形式の２Ｄの輝度パターンを生じ、一緒に、ある程度複雑な輝度パターンを形成する。リングの符号化を、明るい（１）または“暗い”とすることによって行うことによって、結果として得られる位相のみフィルタ処理化ノットパターンは、人間の眼にはもはや感知できないが、特に、位相のみフィルタ処理をオリジナルリングパターンを再生する逆フィルタ処理した後、コンピュータには容易に識別できる微妙な特徴を取りはじめる。

【0251】

ここで図１９に戻ると、我々は、８ビット識別ワードをノットパターンにおいて符号化し、ノットパターンを位相のみフィルタ処理したことを想像できる。結果として得られる輝度分布は、ある美しさを有するが、眼／脳には容易に分からない重なった波パターンの豪華なタペストリである。〔これに対する例外は、南太平洋島共同体の知識から引き出すことができ、航海者は、原始的な航海手段として、分散され反射された間にある島々の沖の海の波によって発生された、小さく、増加する複雑な海の波パターンを読み取る微妙な技術を学んだと言われている。〕よりよい言い回しの要求に関して、結果として得られる（８６６から得られた）フィルタ処理化ノットパターンのモザイクを、符号化ノットタペストリまたは単にノットタペストリと呼ぶことができる。このノットタペストリの幾つかの基本的な特性は、その発生するモザイクの基本的な回転対称性が保持されることと、一般的に、眼／脳には分からず、したがって、逆問題工学の洗練レベルにおける段階を高め

ることと、画素の格子の利用可能な情報内容の使用において、より能率的である（次の節においてより重要である）ことと、基本的なノット概念８５４および８６４を使用する場合、信号レベルが波状に集中し、したがって視聴者に不快に可視になる“ホットスポット”が発生しないことである。

【0252】

上述した基本的な復号化処理は、符号化処理において使用した位相のみフィルタを逆フィルタ処理する追加のステップを必要とする。この逆フィルタ処理は、画像処理産業においてよく知られている。ノットパターンのスケールが先天的に分かっているとすると、逆フィルタ処理は簡単である。他方で、ノットパターンのスケールが分かっていない場合、このスケールを見つける追加のステップが適切である。ノットパターンのスケールを見つける１つのこのような方法は、逆の位相のみフィルタを、復号化している画像の種々のスケールのバージョンに反復的に適用し、顕著なノットパターンを示し始めるスケールバージョンを捜すことである。単体方法のような普通の探索アルゴリズムを、パターンのスケールを正確に見つけるために使用することができる。物体認識の分野も、スケールが分からない物体検出の一般的な表題の下に参照すべきである。

【0253】

ノットタペストリが画像画素格子を覆う能率についての追加点の順番である。万能画像コード化のノットタペストリ方法の大部分の用途は、完全に符号化されたタペストリ（すなわち、埋め込まれたＮビット識別ワードを有するタペストリ）の用途を、比較的低輝度レベルにおいて、ソース画像中に置く。実際の言葉において、符号化タペストリの輝度スケールが、例えば、代表的な２５６グレイスケール画像において－５グレイスケール値から５グレイスケール値で変化し、ここで、値の優勢は－２ないし２となる。これは、ノットタペストリが感知しうるビット切断エラーを受ける単に実際的な方法をもたらす。例として、完全な２５６グレイレベル画像を良好に使用し、これを輝度において係数２０によってビット切断ステップを含むスケールダウンをし、このビット切断バージョンを輝度において同じ係数２０によって再スケーリングし、その結果を逆の位相のみフィルタ処理して構成されたノットタペストリを想像する。結果として得られるノットパターンモザイクは、オリジナルノットパターンモザイクの顕著に劣化したバージョンとなる。このすべてを持ち出す点は、以下の通りである。簡単に規定されるが、実際にはノットタペストリ方法の実現化における設計の種々の自由パラメータを選択する工業的タスクに挑戦し、最終的な目的は、ノットタペストリのある予め規定された可視度許容差内で、Ｎビット識別ワードについての情報の最大量を通過させることである。前記自由パラメータは、画素における要素的リングの半径と、Ｎすなわちリングの数と、画素におけるノットパターンの中心から要素的リングの中心までの距離と、あるノットパターンの他のノットパターンとの詰め込み規準および距離と、ひもの織り方に関するルールと、ノットモザイクに使用すべき位相のみフィルタの形態および形式とを含むが、これらに限定されない。このようなパラメータを、これらの選択において助けになるコンピュータ最適化ルーチンに供給することが望ましい。これは、含まれる多くの非線形自由パラメータにより、科学よりも芸術として始まる。

【0254】

位相のみフィルタ処理の使用における付随する注意は、リングパターンの検出において援助することができることである。前記復号化プロセスの逆のフィルタ処理は、ノットタペストリを付加する、下にあるソース画像を“曖昧”にする傾向があり、同時に、リングパターンを“フォーカスする”傾向がある。ソース画像の曖昧化がなく、現れるリングパターンは、代表的な画像の鮮明な特徴に“対抗”する、より困難な時間を有する。前記復号化手順は、他の節において説明した勾配しきい値化方法も使用すべきである。簡単に、これは、ソース信号が輝度において我々の署名信号より大幅に大きいことが分かっている場合、復号化している画像は、署名信号の信号レベルをソース信号に対して上昇させるサービスにおいて、より高い勾配領域しきい値を有することができる方法である。

【0255】

上述した他の実際的な困難である、２Ｄ　ＦＦＴルーチンおよび代表的なパターン認識ルーチンの相対的な計算上のオーバヘッドに関係する項目（５）に関して、ここに置くが満たされない最初の救済策は、リング輝度の極性を、２Ｄ　ＦＦＴを使用するよりも迅速に認識し、復号化するより簡単な方法を見つけることである。これを除くと、個々のノットパターン（８５０または８５２）の画素範囲を、例えば直径において５０画素とした場合、画像のある部分における簡単な６４掛ける６４画素の２Ｄ　ＦＦＴは、上述したＮビット識別ワードを識別するのに十分であることが分かる。このアイデアは、Ｎビット識別ワードを識別するために、画像全体を使用することが必要であるのと相違して、必要な最小の画像領域を使用することである。

【0256】

他の注意は、画像処理の科学におけるこれらの弁護士がリングの使用を伴うノットタペストリにおける議論を始める代わりに、我々は、ＱＵＡを基礎として機能する２Ｄ輝度分布パターン８７６の使用に真っ直ぐに飛ぶことができる。ベースライン技術としての“リング”という用語の使用は、いずれにしても発明開示に関して適当であるため、幾分教訓的である。より重要なことは、ひょっとすると、逆フィルタ処理後の復号化処理における真の“リング”の使用が、おそらく、代表的なパターン認識ルーチンに入力する最も簡単な形態であることである。

【0257】

ニューラルネットワークデコーダ

信号処理の当業者は、ニューラルネットワークアーキテクチャを用いるコンピュータが、本テクノロジーによって提出された、パターン認識およびノイズにおける微小信号の検出問題に好適であることを認識するであろう。これらの題目における完全な開示は本明細書の範囲を越えており、興味を持った読み手は、例えば、チャーカスキー，ブイ．，“統計学からニューラルネットワーク：理論およびパターン認識用途”，スプリンガー－バーラグ，１９９４；マスターズ，ティ，“ニューラルネットワークによる信号および画像処理：Ｃソースブック”ウィレイ，１９９４；グィオン，アイ．，“ニューラルネットワークシステムを使用するパターン認識における進歩”，ワールド　サイエンティフィック　パブリッシャーズ，１９９４；ニグリン，エイ．，“パターン認識用ニューラルネットワーク”，ウィレイ，１９９３；およびチェン，シー．，“パターン認識用ニューラルネットワークおよびそれらの用途”，ワールド　サイエンティフィック　パブリッシャーズ，１９９１を参照されたい。

【0258】

２Ｄ万能コードII：一次元の場合の単純走査ライン実現化

リング、ノットおよびタペストリーにおける上記節は、確かにその美しさを有するが、含まれるステップの幾つかは、実際的な実現化が、ある用途に対して費用が掛かりすぎてしまう程の複雑さを有するかもしれない。リングおよび良く設計された対称性の概念の粗末な類似は、図９およびオーディオ信号に関連して与えた基本的概念を単純に使用し、これらを画像のような二次元信号に用いるが、例えば、画像における各々の走査ラインが、例えば、１００画素長万能ノイズ信号においてランダムな開始点を有するように行うことである。識別ソフトウェアおよびハードウェアは、回転状態およびスケール係数の完全な範囲を横切る像を質問し、これらの万能コードの“存在”を見つける義務がある。

【0259】

万能商用著作権（ＵＣＣ）画像、オーディオおよびビデオファイルフォーマット

よく知られているように、過多のディジタル画像、ディジタルオーディオおよびディジタルビデオに関するファイルフォーマット標準（および標準でないもの）が存在することは残念である。これらの標準は、一般的に、特定の産業および用途内で形成されており、拡散した創造的ディジタル題材の使用および交換のため、種々のファイルフォーマットが、交互の規律のための闘技場において激しく戦い、そこで今日、我々は、種々の気に入っているフォーマットの熱狂的なファンおよびユーザの事実上のヒストグラムを見る。フォーマット化および圧縮のためのＪＥＰＧ、ＭＰＥＧ標準は、ある計画された産業間の共同

研究が活動しはじめる場合に見ることができる、わずかな例外に過ぎない。

【0260】

オーディオ／ビジュアルのための簡単な万能標準ファイルフォーマットに対する切望は、非常に古い。このような題材の保護に対する切望は、なおさら古い。万能フォーマットの形成に伴う固有の困難に関して、そして、特許開示内のこのような計画の概略の勿体ぶりに関して、本発明者は、これらの方法が、ひょっとすると、一般に認められた世界的な“万能商用著作権”フォーマットを構成する基礎となるなにかと同様に役に立つことができると信じている。弁護士は、このような動物が、宣言によって形成されず、広いニーズ、固執および幸運の能率的な集合を通じて形成されることを知っている。この開示の目的により密接に関係することは、このテクノロジーの用途が、産業標準ファイルフォーマット内の中心的な部分になる場合、利益を得ることである。特に万能コードの使用を、このような標準内に指定することができる。このテクノロジーの商業的習慣の最大限の表現は、不可視署名を行い、信用を著作権保持者に吹き込む知識から来ている。

【0261】

以下は、このテクノロジーの原理がこのような標準に対する触媒として働くことができる理由のリストである。（１）いるとしてもほとんどいない技術的開発者が、経験的データおよびオーディオ／ビジュアル題材の不完全な保護の問題を隔離し、明白にアドレスする。（２）すべての上述したファイルフォーマットは、データについての情報と、データ自体とを、２つの分離して物理的に異なった存在として取り扱っているが、このテクノロジーの方法は、これら２つを１つの物理的存在に結合することができる。（３）このテクノロジーの原理の大スケール用途は、まず第１に、圧縮テクノロジーにおける未来の改善による統合を含む、実際的な標準化作業を必要とし、その結果、標準の基板が存在しなくなる。（４）マルチメディアの発達は、“内容標準”のますます高いレベルを論じる、テキスト、画像、サウンドおよびグラフィックスを含む“内容”と呼ばれるデータの属性クラスを形成した。（５）著作権保護テクノロジーおよびセキュリティ特徴をファイルフォーマット標準に直接結合することは、長い間遅れている。

【0262】

万能標準の要素は、前記ヘッダ証明方法の鏡像的な特徴を必ず含み、ここで、ヘッダ情報を、直接にデータ内の署名コードによって識別する。また、万能標準は、完全に秘密のコードおよび公開コードの混成使用をどのように混じり合わせるかの概略を述べる。したがって、公開コードを洗練された著作権侵害者によって“取り除かれた”場合、秘密コードは元のままである。万能標準は、不可視署名が、ディジタル画像およびオーディオが発展するにつれてどのように発展するかを指定する。したがって、所定の画像を、いくつかのソース画像を基礎として形成した場合、前記標準は、古い署名をどのように何時取り除き、新たな署名によって置き換えるかと、前記ヘッダかこれらの発展の記録を残すかどうかと、署名自体がある種の記録を保つかどうかとを指定する。

【0263】

画素対突起

本開示の大部分は，Ｎビット識別ワードの基本的キャリヤである画素に焦点を置いている。１つの“マスタコード信号”の使用を論じる節は、各々のそしてすべの画素をＮビット識別ワードにおける固有のビットプレーンに本質的に“割り当てる”点まで行っている。

【0264】

多くの用途に関して、インチ当たり３００ドットの解像度におけるインクを基礎とする印刷の用途である一例によれば、原始的なディジタル画像ファイルにおける画素が実際に（例えば、一枚の紙においてディザ化されたインクの）染みになる。しばしば、オリジナル画素の容量を輸送する孤立した情報は、隣接する画素が、オリジナル画素の幾何学的に規定された空間にこぼれることによって妥協される。当業者は、これを、簡単な空間フィルタ処理および、ブラーリングの種々の形態として認識するであろう。

【0265】

このような情況において、単に１つの画素よりも、特定の画素の極めて局所的なグループを、Ｎビット識別ワードにおける固有のビットプレーンにより有利に割り当てることができる。最終的な目的は、単に、署名信号エネルギのより多くを、より低い周波数に予め集中し、大部分の実際的な実現化が、より高い周波数を迅速に取り除く、または軽減することを実現することである。

【0266】

素朴なアプローチは、１つの割り当てられた画素を変調するよりも、変調すべきすべての画素の２掛ける２のブロックに同じ基本的な署名グレイ値を割り当てることである。より上等なアプローチを図２１において示し、ここで画素グループのアレイを示す。これは、配置の大きなクラスの特定の例である。このアイデアは、画素の特定の小さな領域をＮビット識別ワードにおける所定の固有ビットプレーンに関係させ、このグループ化が、ビットプレーン間の画素を実際的に共有する（前記画素の２掛ける２のブロックの場合のように、画素を共有する必要がないとしても）ことである。

【0267】

図２１に示したものは、一例の正規化重み付けを有する、画素の３掛ける３アレイである（正規化→合計１になる重み）。このテクノロジーの方法は、１つの画素におけるよりも、単位として、この要素的“突起”において動作する。この例において、署名信号の拡張により、格納することが必要なマスタコード値の数において４倍の減少があることが分かる。不可視署名における配置に対するこの“突起アプローチ”の用途は、先天的に既知の多量のブラーリングを経験し、この激しいブラーリング後においても正確な識別を求められるいかなる用途をも含む。

【0268】

このテクノロジーのステガノグラフィ的使用におけるその他

本開示の初めの節において言及したように、技術および科学としてのステガノグラフィは、このテクノロジーに対する一般的な先行技術である。ここで、立場を逆にし、ここまで冒険してきた読み手にはすでに疑いなく明白であるように、このテクノロジーの方法を、ステガノグラフィを行う新規の方法として使用することができる。（なるほど、ここまでの考察のすべては、ステガノグラフィの種々の形態および実現化を調査することに関係している）。

【0269】

本節において、我々は、ステガノグラフィを、メッセージを点Ａから点Ｂに伝える必要性として考え、このメッセージを、一般的に独立の経験的データ内に本質的に隠されているとする。遠隔通信の産業における誰かが証明できるため、メッセージを伝える目的の範囲をかなり広くする。恐らく、これらのメッセージをなんらかの数の慣例的で簡単なチャネルを経て送信するよりも、純粋な趣味の他に、ある例外的な必要性があるであろう。ステガノグラフィにおける過去の文献および製品宣伝は、特にこのような例外的な必要性を、メッセージがまさに送られている事実を隠すことに対する要求としているかもしれない。他の可能な必要性は、慣例的な通信チャネルが直接利用できないか、費用的に禁止されるとして、すなわち、メッセージの送り手が彼等の符号化経験的データをどうにかして“送信する”ことができることである。この開示は、参照により、ステガノグラフィを用いることができる無数の使用におけるすべての以前の考察を含み、本発明者がまだ説明していない以下の使用を追加する。

【0270】

第１のこのような使用は、きわめて簡単である。その中でメッセージを輸送する経験的データについてのメッセージを輸送することが必要である。ある以前のステガノグラフィ実行者がすでにこの冗談を利用していないことが、次は不可能であるとしても、ささいな冗談は、媒体が真にメッセージである。経験的データについての情報をその経験的データ内に直接配置することにおけるある考察は、ヘッダを交換することにおける節と、“ボディア”の概念とにおいて既にカバーされている。

【0271】

経験的データについてのメッセージをそのデータ内に直接配置することの利点は、データオブジェクトの、以前の２つのクラスよりも、ただ１つのクラスが存在することである。どのような２クラスシステムにおいても、２つのクラスが無関係になるか、一方のクラスが他方のクラスがそれについて知ることなしに汚染される危険性が存在する。具体的な例は、本発明者が“装置独立命令”と呼ぶものである。

【0272】

無数の機械データフォーマットおよびデータファイルフォーマットが存在する。このフォーマットの過多は、万能データ交換に向かう進歩を妨害するそのパワーと、ある機械は、他の機械ができることと同じことを行っていることとにおいて悪名が高い。創始者がデータの第２クラス（すなわちヘッダ）に用いたかもしれない命令は、これらの命令を認識するようにした機械に少しも適合しないかもしれない。フォーマット変換を行った場合、決定的な命令が、この進路に沿って取り除かれるか、混乱するかもしれない。ここで開示した改善を、命令およびメッセージを認識するために読み出し機械によって必要とされるすべてが、経験的データにおける標準化“認識アルゴリズム”を行うものとなるように、特定の命令を経験的データに直接“封印する”方法として使用することができる（もちろん、機械は、経験的データ特性を少なくとも“読む”ことができる）。すべての機械は、このアルゴリズムを、これらが選択したなんらかの古い方法で、なんらかのコンピュータ、またはこれらが必要とする内部データフォーマットを使用して実現することができる。

【0273】

この装置独立命令方法の実現化は、一般的に、メッセージに封印されたものの著作権侵害または不正な除去の問題を考慮していない。恐らく、埋め込まれたメッセージおよび命令は、題材の基本値および機能における中心的な大切な部品となるであろう。

【0274】

本テクノロジーの一種のステガノグラフィ的な使用の他の例は、ユーザ共同体の利益のための万能使用コードの埋め込みである。伝達されている“メッセージ”を、単に、経験的情報の正当な使用および支払いを望むユーザに対して所有権を認める登録シリアル番号とすることができる。このシリアル番号は、所有者の名前や、値付け情報や、請求情報、等を含む創造的特性の莫大な登録に見出し付けすることができる。前記“メッセージ”を、所定の題材に関する自由および公的な使用の許可とすることもできる。同様の所有者識別および使用インデックス化を、ヘッダのような２クラスデータ構造方法において達成することができるが、このテクノロジーの１クラスシステムの使用は、前記１クラスシステムが、ファイルフォーマット変換、ヘッダ互換性、内部データフォーマット問題、ヘッダ／ボディアーカイビング問題、および媒体変化を気にしないという、前記２クラスシステムを越えるいくらかの利点を提供することができる。

【0275】

完全に正確なステガノグラフィ

本発明者に現在既知の先行技術のステガノグラフィ的技術は、一般的に、メッセージを伝達する完全に決定論的、すなわち“正確”な処方を含む。すなわち、これは、完全に正確に伝達すべき所定のメッセージに関して、情報の受け手は、送り手によって送られた正確なディジタルデータファイルを受ける必要があり、ビットエラーまたはデータの“損失”を許容することが、基本的な仮定である。定義により、経験的データにおける“損失的”圧縮または伸張は、このようなステガノグラフィ的方法を無効にする。（上述したコマツの仕事のような先行技術は、ここでは例外とする）。

【0276】

このテクノロジーの原理を、ステガノグラフィ固有の正確な形態として利用することができる。先行技術またはこのテクノロジーのこのようなステガノグラフィの正確な形態は、“ディジタル署名”および／またはＤＳＳ（ディジタル署名標準）の比較的新しい技術と、所定の経験的データの受け手が、情報のどのビットも受けたファイルにおいて変化していないことを最初に確かめることができ、したがって、含まれる正確なステガノグラフィ的メッセージが変化していないことを確かめることができるように結合されることが暗

示される。

【0277】

正確なステガノグラフィ的システムにおいてこのテクノロジーの原理を使用する最も簡単な方法は、マスタ雪状コードがゼロを含むことを許可されない、上述した“設計された”マスタノイズ計画を使用することである。情報の送り手および受け手の双方が、前記マスタ雪状コード信号およびオリジナル非符号化オリジナル信号の双方にアクセスする必要がある。符号化信号の受け手は、単に、オリジナル信号を減算して差信号を与え、前記差信号とマスタ雪状コード信号との間の簡単な極性検査の技術が、データ標本毎に、伝達されたメッセージを同時に１ビット発生する。恐らく、グレイ値範囲の“レール”に近い値を有するデータ標本は、（８ビット深さの経験的データにおいて値０、１、２４５および２５５のように）取り除かれる。

【0278】

統計的ステガノグラフィ

ステガノグラフィ的に埋め込まれたデータファイルの受け手に対する、オリジナル信号へのアクセスを有する必要性は、本発明者が“統計的ステガノグラフィ”と呼ぶものに頼ることによって取り除くことができる。このアプローチにおいて、このテクノロジーの方法を、埋め込まれたメッセージを探索する経験的データセットの読み出しを支配する単純な先天的ルールとして用いる。この方法は、ＤＳＳによるようなデータファイルの完全性を識別する先行技術の方法と組み合わせても良好に使用できる（例えば、ワルトン，“不安定な新時代のための画像認証”，ドクター　ドブズ　ジャーナル，１９９５年４月，標本ずつ、ビットずつ、ディジタル画像の完全性を識別する方法に関する１８ページを参照されたい）。

【0279】

統計的ステガノグラフィは、送り手および受け手の双方が、同じマスタ雪状コード信号へのアクセスを有する。この信号を、完全にランダムで確実に双方のパーティに送ることができ、または、より大きい疑似ランダムマスタ雪状コード信号を発生する、共有され安全に送信されたより低いオーダのキーによって発生することもできる。メッセージの１６ビットの固まりは、経験的データの隣接する１０２４標本ブロック内で伝達され、受け手は、本開示において概要を述べたようなドット積復号化方法を使用することが、先天的に規定されている。情報の送り手は、ドット積アプローチが正確な１６ビット値を実際に発生することを、予め検査する（すなわち、送り手は、キャリヤ画像とメッセージ信号との間のクロストークが、ドット積動作がどの１６ビットの望ましくない反転も発生するようなものでないことを予め検査する）。ある一定の数１０２４の標本ブロックを送信し、したがって１６ビットのメッセージを同じ数の回数送信する。ＤＳＳテクニックを使用し、送信されたデータがディジタル形態における存在に対してのみ既知である場合、メッセージの完全性を識別することができ、それとは相違して、内部チェックサムおよびエラー訂正コードを、データがその送信において変化および変換されるかもしれない情況において送信することもできる。この後者の場合において、所定のメッセージ内容サイズに対して標本のブロックをより長くする（単に例として、１６ビットメッセージ固まりに対して１０Ｋ標本のようにする）ことが最適である。

【0280】

エラー訂正ステガノグラフィの話題における時間を続けると、ここに開示された多くの復号化テクニックは、符号化データによって増加した画素（または突起）を、符号化データによって減少したこれらから識別する原理において動作することが認識されるであろう。これらのポジティブおよびネガティブな場合の識別は、デルタ値（例えば、符号化画素と対応するオリジナル画素との差）がゼロに近づくにつれて増加的に困難になる。

【0281】

類似した情況は、曖昧な中間グランドが２つの所望の信号状態（例えば、＋／－１）に分離する、特定のモデム送信技術において発生する。この中間グランドの誤った判断から得られるエラーは、時々“ソフトエラー”と呼ばれる。モデム技術およびこのような問題

が発生する技術からの原理を、同様に、現在の情況におけるこのようなエラーの軽減に用いることができる。

【0282】

１つのアプローチは、各々のデルタ測定の“信頼性”に重み付けすることである。画素（突起）が明らかにある状態または他の状態（例えば、＋／－１）をもたらす場合、その“信頼性”をハイであると言い、比例してより大きい重み付けを与える。反対に、画素（突起）がその判断において比較的曖昧である場合、その信頼性は相応してより低く、比例的により小さい重み付けを与える。その信頼性値に従って各々の画素（突起）からのデータを重み付けすることによって、ソフトエラーの影響を大幅に減少させることができる。

【0283】

このような信頼性重み付けを、他のエラー検出／訂正計画に対する有用な補助として使用することもできる。例えば、既知のエラー訂正多項式において、上述した重み付けパラメータを使用し、エラーの場所の多項式を基礎とする識別をさらに鋭くすることができる。

【0284】

ベクトルグラフィックスおよび極めて低いオーダのインデックス化グラフィックスにおける“ノイズ”

この開示の方法は、一般的に、“経験的データ”の存在を仮定し、これは、ほとんど定義によってそれらに含まれるノイズを有する信号を言い表す他の方法である。一般的に、先天的にノイズを有するとは考えられない二次元グラフィックスの２つのクラス、すなわち、ベクトルグラフィックスおよび特定のインデックス化ビットマップ化グラフィックスが存在する。ベクトルグラフィックスおよびベクトルグラフィックファイルは、一般的に、コンピュータまたはプリンタが、直線、曲線および形状をどのように描写するかについての正確な命令を含むファイルである。このようなファイルにおける１ビット値の変化は、極めて大雑把な例として、円を四角に変えるかもしれない。すなわち、一般的に、これらのファイル内に利用する“先天的ノイズ”が存在しない。インデックス化ビットマップ化グラフィックスは、ＰＣコンピュータにおける初期のＣＧＡでぃすぷれいちおける１６のように、一般的に少ない数の色またはグレイ値から成る画像に属する。このような“極めて低いオーダ”のビットマップ化画像は、通常、自然界のカメラによって撮ったディジタル画像の試みられた表示において使用するよりも、グラフィックスおよびマンガを表示する。これらの形式の極めて低いオーダのビットマップ化グラフィックスも、一般的に、古典的なセンスの言葉における“ノイズ”含むとは考えられない。例外は、“ノイズ”の概念が依然として有効であり、このテクノロジーの原理が依然として有効である、インデックス化グラフィックファイルが、ＧＩＦ（コンピュサーブのグラフィック交換フォーマット）によるような自然画像を表現しようとする場合である。これらの後者のフォーマットは、しばしば、（点描印刷およびカラー新聞印刷と同様の）ディザリングを使用し、実物に近い画像を達成する。

【0285】

この節は、慣例的に“ノイズ”を含まない２次元グラフィックスのこのクラスを考察する。この節は、このテクノロジーの原理を、どのように依然としてある方法においてこのような創造的題材に適用できるようにするかについての簡単な様子を取り上げる。

【0286】

このテクノロジーの原理をこれらの“無ノイズ”グラフィックスに用いる最も簡単な方法は、これらを、このテクノロジーの原理の用途に従う形態に変換することである。多くの言葉が、この産業において、ベクトルグラフィックをグレイスケールの画素を基礎とするラスタ画像に変換するような、ベクトルグラフィックの“リッピング”を含む、この変換に使用されている。アドビによるフォトショップのようなプログラムは、ベクトルグラフィックをＲＧＢまたはグレイスケールディジタル画像に変換するこのような内部ツールを有する。一度これらのファイルをこのような形態に変換すると、このテクノロジーの原理を簡単な方法で適用することができる。同様に、極めて低いインデックス化ビットマッ

プを、ＲＧＢディジタル画像または同等物に変換することができる。ＲＧＢ領域において、前記署名を適切な比において３つのカラーチャネルに用いることができ、または、ＲＧＢ画像を、アドビのフォトショップソフトウェアにおける“ラブ”のようなグレイスケール／クロマフォーマットに簡単に変換することができ、前記署名を“明るさチャネル”に用いることができる。ビデオテープ、ＣＤ－ＲＯＭ、ＭＰＥＧビデオ、ディジタル画像、および印刷のような配布媒体の大部分が、このテクノロジーの原理の用途に従う形態であるため、ベクトルグラフィック形態および極めて低いオーダのグラフィック形態からのこの変換は、何らかのイベントにおいてしばしば行われる。

【0287】

このテクノロジーの原理をベクトルグラフィックスおよび極めて低いオーダのビットマップ化グラフィックスに用いる他の方法は、眼に対してノイズとして現れるこれらの先天的なグラフィックフォーマットに対する特定の特性が存在することを認識することである。最初の例は、所定のラインまたは形状が描かれているまたは描かれていない場所、または正確に、ビットマップが緑から青に変化する場所の境界および輪郭である。大部分の場合において、このようなグラフィックスの人間の視聴者は、グラフィックオブジェクトの正確な輪郭の微細で組織的な変化による“変調署名信号”のいかなる試みにも鋭く気付くであろう。それにもかかわらず、このような署名の符号化は、実際に可能である。このアプローチと、この開示の大部分において開示されているものとの差は、ここでは、署名を、純粋に別個に形成したり信号に追加するよりも、最終的に所定のグラフィックにおいてすでに存在するものから得なければならないことである。この開示は、それにもかかわらずここで可能性を指摘する。基本的なアイデアは、輪郭、右方接触または左方接触、上方接触または下方接触を、Ｎビット識別ワードを伝達することのように変調することである。ノイズが、所定の輪郭に垂直のある方向または他の方向のランダムな空間シフトの記録であるとしても、変化する輪郭の場所は、類似のマスタノイズ画像に含まれる。Ｎビット識別ワードのビット値を、用いられた変化とマスタノイズ画像に記録された変化との同極性検査を使用して、符号化し、読み出す。

【0288】

本テクノロジーの原理を基礎とするプラスチッククレジットおよびデビットカードシステム

プラスチッククレジットカードと、より最近ではデビットカードおよびＡＴＭキャッシュカードとの使用における発展は、ほとんど前書きを必要としない。ここでこれらの金融手段の詐欺および不正使用の長い歴史について多く議論することも必要ない。クレジットカードホログラムの発展と、その後の偽造物の発展とは、プラスチックカードセキュリティ手段および不正な対抗策のギブアンドテイクの歴史的な例として適している。この節は、それ自体が、このテクノロジーの原理を、選択的に高度に耐詐欺的でありながら費用効果的なプラスチックカードを基礎とする金融ネットワークにおいてどの様に実現できるかに関係する。

【0289】

偏在的なプラスチック経済に関する所望の特徴の基本的なリストは、以下の通りである。１）所定のプラスチック金融カードは、偽造することが完全に不可能である。２）試みられた偽造カード（良く似ている）は、処理環境においてまったく機能することができない。３）著作権侵害志望者によって妨害された電子処理は、どのようにも有効とならず、または再使用可能にならない。４）実際の有効なカードの物理的盗難の事象において、盗難者がそのカードを使用するのを依然として強力に邪魔をする。５）金融カードシステムの全体的な経済的費用が、現在の国際的クレジットカードネットワークと等しいかまたは低い、すなわち、処理あたりのすべての負担される費用が、ネットワークの実現化に対するより高い利益マージンを与える現在の標準と等しいかまたは低い。完全に実現化戦略と共に含まれる工業および社会問題の詳細な分析を必要とする項目５を別として、以下のこのテクノノロジーの原理の使用は、上記リストを、項目５でさえも、良好に達成することができる。

【0290】
図２２ないし２６は、続く書かれた材料と共に、図２６において“詐欺を無視しうるキャッシュカードシステム”と呼ばれるものを共に要約している。このシステムの詐欺防止特徴が、タイトルにおいて強調されている理由は、その詐欺および付随する損失収益が、今日のプラスチックカードを基礎とする経済において中心的な問題であることである。現在のシステムに対するこのシステムの差別的な利点および欠点を後に考察し、説明的な実施形態を与える。
【0291】
図２２は、各々そして全てのユーザに対して固有の基本的偽造不可能プラスチックカードを説明する。ディジタル画像９４０は、カードのユーザを撮ったものである。図２６に示す中央会計ネットワーク９８０内に接続されたコンピュータは、ディジタル画像９４０を受け、（図２４を取り巻いて説明するような）その処理の後、次にパーソナルキャッシュカード９５０に印刷される最終的なレンダリングされた画像を発生する。さらに図２２に示すものは、この場合においてバーコード９５２である簡単な識別マーキングと、図２３に示す読み取り装置９５８における走査許容差を単純化するのを補助することができる任意の位置基準とである。
【0292】
短い話は、パーソナルキャッシュカード９５０は、その個々のカードに固有の極めて大量の情報を実際に含むことである。はめ込まれた磁気ノイズ信号のような同じ原理を磁気ストリップに確実に用いることができるとしても、磁気ストリップは含まれない（クレジットカードにおける磁気ストリップの“指紋”における以前の考察を参照されたい。ここでは、指紋は、受け身に対して目立ち、予防的である。）。なんらかのイベントにおいて、パーソナルキャッシュカード９５０における画像内の固有情報を、基本会計情報と共に図２６の中央会計ネットワーク９８０に格納する。破ることのできないセキュリティの基本は、処理中、中央ネットワークが、カードにおいて含まれる全体の情報の小さな割合を疑うことのみを必要とし、どのような２つの処理における同じ正確な情報も疑う必要がないことである。数千または数千の内の数十でないとしても数百の固有で保障された“処理証拠”が、一枚のパーソナルキャッシュカードに含まれる。暗号化された、または暗号化されていない処理の伝送に干渉しようとする著作権侵害志望者は、その後、情報が役に立たないことを見つける。これは、その全体において、繰り返してアクセスすることを必要とする１つの複雑で完全な（一般的に暗号化された）“キー”を有するシステムとは違うものである。他方でパーソナルキャッシュカードは、一度、数ミリ秒内で使用することができ、その後（いわば）破棄される数千の別個の保障されたキーを含む。中央ネットワーク９８０は、前記キーの痕跡を保持し、すでに使用されており、有していないことを知る。
【0293】
図２３は、それらしく見えるかもしれない、代表的な売り点読み取り装置９５８を示す。明らかに、このような装置は、現在のキャッシュレジスタシステム、ＡＴＭシステムおよびクレジットカードの磁気ストライプ読み取り装置と、コストにおいて同等にまたは安価に製造可能である必要がある。光学的走査、画像処理およびデータ通信部品の内部は、図２３において示しておらず、これらは、今後説明すべきものであり、恐らく当業者の能力内である機能を実行する通常の工業的設計方法に単に従うものである。読み取り装置９５８は、（一般的に、物理的なカードの盗難が発生した後）セキュリティのもう１つの慣例的なレイヤを追加する通常のパーソナル識別番号システムをこのシステムの全体的な設計に結合できることを示す数字タッチパッド９６２を有する。ユーザの写真の使用が、盗んだ後の不正使用を防ぐための強力な（かつ増加的に一般的な）セキュリティ特徴であることも指摘すべきであろう。カードの形状を真似し、走査用のセンタリング機構として重ねる光学的ウィンドウ９６０のような機能的要素を示す。恐らく、所有者の中央商業コンピュータシステムか、可能なら中央ネットワーク９８０に直接接続されたデータラインケーブル９６６も示す。このような読み取り装置を、購入された項目の通常の計算を行うキ

ャッシュレジスタに直接接続してもよい。カードの未加工の走査のような非電子信号がユニットから流出するかもしれないような、ファラデーケージの形式のような読み取り装置９５８の構成は、ひょっとするとセキュリティにおいて過剰である。読み取り装置９５８は、後に説明するドット積演算の高速の計算において援助するディジタル信号処理ユニットを好適には含む必要がある。図２５とその考察において概説した“認識”ステップにおいて使用される多数の空間パターン（直交パターン）を格納する局所的読み出し専用メモリも含むべきである。図２３に示すように、プラスチックカードを使用する消費者は、単に、彼らのカードを前記ウィンドウ上に置き、商取引に関して支払う。ユーザは、彼ら自身に関して、ＰＩＮ番号を使用したいかどうかを選択することができる。図２５の信号処理ステップが、効果的に並列ディジタル処理ハードウェアによって満たされる特性の場合、購入の許可は、おそらく数秒以内に起こる。

【0294】

図２４は、ユーザの未加工ディジタル画像９４０を、より有用な情報内容および固有性を有する画像に処理する１つの方法における大まかな様子を取り上げる。事実上、未加工ディジタル画像それ自体を以下の方法において使用することができるが、追加の直交パターンの該画像への配置は、システム全体をかなり増加させてしまうかもしれないことを、明らかに指摘すべきである。（直交は、所定のパターンを他の直交パターンによって乗算した場合、結果として得られる数がゼロになることを意味し、ここで、“パターンの乗算”は、ベクトルドット積の意味であり、これらはすべて、ディジタル画像処理の技術においてよく知られている言葉および概念である。）図２４は、コンピュータ９４２が、未加工画像９７０の質問の後、未加工画像９７０に付加することができ、実際のパーソナルキャッシュカード９５０に印刷される画像であるより固有の画像を発生する、マスタ雪状画像９７２を発生することを示す。画像における全体的な効果は、画像を“テクスチャ化”することである。キャッシュカードの場合において、マスタ雪状パターンの不可視性は、商用画像ほど高い要求はされず、マスタ雪状画像をある程度より明るく保つ唯一の規準は、ユーザの画像を曖昧にしないことである。中央ネットワーク９８０は、最終的な処理された画像をユーザの口座の記録に格納し、この固有で安全に保持された画像を、高度に保障された“破棄商取引キー”のキャリヤとする。したがってこの画像は、ネットワーク全体におけるすべての適切に接続された売り点の場所に対して“利用可能になる”。理解されるように、売り点場所は、この画像の知識を持たず、単に、中央ネットワークからの質問に答える。

【0295】

図２５は、代表的な商取引の順序を進む。この図を、第１の段が売り点読み取り装置９５８によって行われるステップであり、第２の段がデータライン９６６上で通信される情報伝送ステップを有し、第３の段がユーザの口座およびユーザの固有パーソナルキャッシュカード９５０についての保障された情報を有する中央ネットワーク９８０によって行われるステップである、字下がりによって並べる。このようなシステムの工業的実現化において通常に行われるため、これらのステップの実現化においていくらかの一致する可能性が存在するが、これらのステップをイベントの一般的な直線的順序に従って並べた。

【0296】

図２５のステップ１は、光学的ウィンドウ内のパーソナルキャッシュカード９５０の標準的な“走査”である。これを、前記ウィンドウを走査する線形光センサを使用して、または、ＣＣＤのような２次元光検出器アレイによって行うことができる。結果として得られる走査を、グレイスケール画像にディジタル化し、光学的画像化システムの設計において一般的であるような、“フレームグラッバ”のような画像フレームメモリバッファに格納する。一度カードが走査されると、第１画像処理ステップが、恐らく、４つの基準中心点９５４を位置決めし、これらの４つの点をすべてのさらなる画像処理動作をガイドするために使用する（すなわち、前記４つの中心は、パーソナルキャッシュカードにおける対応するパターンおよびバーコードを“正しく揃える”）。次に、バーコードＩＤ番号を、一般のバーコード読み取り画像処理方法を使用して抽出する。一般的に、ユーザの口座番

号は、このステップにおいて決定される。

【0297】

図２５のステップ２は、ＰＩＮ番号の任意の印刷である。恐らく、このようなことを覚えている時間がないユーザや、誰も彼らのキャッシュカードを盗まないと確信しているユーザを除く大部分のユーザは、この特徴を有することを選択するであろう。

【0298】

図２５のステップ３は、データラインを経て中央会計ネットワークに接続し、最新の通信ネットワークにおいて一般的な通常の通信ハンドシェークを使用することを行う。このシステムのより洗練された実施形態は、光ファイバデータリンクのユーザのように、標準的な電話線の必要性を取り除くが、ここで我々は、庭の種々のベルトーン電話を仮定し、読み取り装置９５８が中央ネットワークの電話番号を忘れないと仮定することができる。

【0299】

基本的な通信が確立した後、ステップ４は、売り点位置がステップ１で見つけたＩＤ番号を、恐らく、ＰＩＮ番号の（セキュリティを増すために、より偏在的なＲＳＡ暗号化方法を使用するように）暗号化したものと共に送信し、売り点読み取り器９５８を操作する商人における基本情報と、通貨単位における必要な商取引の量とを付加する。

【0300】

ステップ5は、中央ネットワークが、ＩＤ番号を読み取り、ユーザ口座の実際のメモリ位置に従って情報をルーティングし、その後、ＰＩＮ番号を照合し、口座残高が前記商取引に支払うために十分であることを検査することを行う。この方向に沿って、中央ネットワークは、商人の口座にもアクセスし、有効であることを検査し、予測されるクレジットの準備をする。

【0301】

ステップ６は、ステップ５がすべての計算を通過したという仮定によって開始するステップ５が通過していない場合の、非承認を承認に送る出口ステップは図示しない。すべてを確かめた場合、中央ネットワークは、１６の番号の２４の組を発生し、これらのすべての番号は相互排他的であり、一般的に、大きいが、明確に有限の番号の範囲が存在し、そこから選択する。図２５は、６４Ｋまたは６５５３６数である範囲を示す。実際には、どのような実際の番号とすることもできる。したがって、２４の組のある組は、例えば、番号２３１９９、５４１４２、１１００７、２８５４、６１９３２、３２８７９、３８１２８、４８１０７、６５１９２、５２２、５５７２３、２７８３３、１９２８４、３９９７０、１９３０７および４１０９０を有してもよい。次の組を同様にランダムにするが、前記ある組の番号をここでは前記２４の組を通じて立入禁止とする。したがって、中央ネットワークは、（１６×２４×４バイト）の番号すなわち７６８バイトを送る。番号の実際の量は、セキュリティ対送信速度問題の工業的最適化によって決定される。これらのランダム番号は、実際には、中央ネットワークにとって既知であり、売り点読み取り器のすべてにおけるメモリに不変に格納されている６４Ｋの一般的に先天的に規定されている直交パターンに対するインデックスである。理解されるように、盗人志望者のこれらのパターンの知識は、役に立たない。

【0302】

ステップ7は、次に、基本的な“先に進む承認”メッセージを読み取り器９５８に送信し、１６のランダムインデックス番号の２４の組も送る。

【0303】

ステップ８は、前記読み取り器が、すべてのこれらの番号を受信し、格納することを行う。次に、前記読み取り器は、その局所的マイクロプロセッサと、注文設計された高速ディジタル信号処理回路網を使用し、中央ネットワークがカードの画像の真実性を試験する“１回キー”として中央ネットワークに送り返される２４の別個の浮動小数点数を得る意図と共に、すべての番号の２４の組を通じて進む。前記読み取り器は、これを、最初に、所定の組の１６のランダム番号により示された１６のパターンを合計し、次に、結果として得られた複合パターンと、カードの操作された画像との通常のドット積演算を行う。こ

のドット積は、（簡単に、我々が浮動少数点数と呼ぶことができる）１つの数を発生する。前記読み取り装置は、すべての２４の組を通じて同様に進み、２４の浮動少数点数の固有の列を発生する。

【0304】

ステップ９は、次に、前記読み取り装置が、これらの結果を前記中央ネットワークに送り返すことを行う。

【0305】

ステップ１０は、次に、前記中央ネットワークが、これらの帰ってきた２４の数において検査を行い、恐らく、それ自体正確に同じ計算を、中央ネットワークがそれ自体のメモリに有する前記カードの格納された画像に行う。輝度スケール問題を取り除くために、前記読み取り装置によって送られた数を、集められた２４のドット積の最も高い絶対値をそれ自体（その無符号値）によって割ることができることを意味する“規格化”することができる。前記戻ってきた数と、中央ネットワークの計算値との結果として得られる一致は、所定の許容差内で、カードが有効である場合に満足し、カードが偽物である場合か、カードが未加工複製である場合、外れる。

【0306】

ステップ１１は、次に、前記中央ネットワークが、商取引が承認されたかどうかのワードを送り、客に、彼らの購入したものと一緒に家に帰れることを知らせることを行う。

【0307】

ステップ１２は、次に、商人の口座に商取引額をどのように記入するかを明瞭に示す。

【0308】

上述したように、このプラスチックカードの第１の利点は、明らかに現在のシステムに対する高い費用である詐欺を大幅に減少させることである。このシステムは、物理的カードが盗まれるか、極めて注意深く複製された場合に対してのみ詐欺の可能性を減少させる。これらの場合の双方において、ＰＩＮセキュリティおよびユーザ写真セキュリティ（低い賃金の事務員が署名を分析するよりも高いセキュリティの既知のシステム）が依然として残っている。カードを複製する試みは、カードの“一時的な窃盗”によって行われるはずであり、写真品質の複製装置と、単純でない磁気カード磁気ストライプ読み取り装置とを必要とする。このシステムは、最近の２４時間高度リンク化データネットワークに基づいている。商取引の不正な監視は、商取引が暗号化されているかどうかを部分的に使用しない監視を行う。

【0309】

クレジットおよびデビットカードシステムを含む商取引のセキュリティを増す前述のアプローチは、いかなる写真を基礎とする識別システムにも容易に拡張されることは、明らかであろう。さらに、本テクノロジーの原理を、写真ＩＤ文書の変化の検出と、このようなシステムの信頼性およびセキュリティの一般的な増大に用いることもできる。この関係において、例えば、パスポート、ビザ、永住許可証（グリーンカード）、運転免許証、公務員身分証明書、または民間企業身分証明バッジとすることができる、写真ＩＤカードまたは文書１０００を示す、図２８を参照する。便利のため、このような写真を基礎とする身分証明文書を、総体的に写真ＩＤ文書と呼ぶ。

【0310】

写真ＩＤ文書は、文書１０００にはりつけられた写真１０１０を含む。印刷された人間が読める情報１０１２が、文書１０００において写真１０１０に近接して含まれる。“バーコード”として既知のような機械が読める情報を、前記写真に近接して含んでもよい。

【0311】

一般的に、写真ＩＤ文書を、文書の偽造（例えば、オリジナルの写真を他の写真と交換する）は、カードに顕著な損傷を引き起こすであろう。それにもかかわらず、熟練した偽造者は、存在する文書または不正製造写真ＩＤ文書を、検出することが極めて困難な方法において交換することができる。

【0312】

上述したように、本テクノロジーは、写真ＩＤ文書の使用に関係するセキュリティを、写真画像に符号化情報（この情報を視覚的に感知可能にしてもしなくてもよい）に付加し、それによって、文書１０００に現れる印刷された情報１０１２のような、人物に関係する他の情報により写真画像の訂正を容易にすることによって拡大する。

【0313】

ある実施形態において、写真１０１０を、図２２－２４に関係して上述したようなマスタ雪状画像を付加した未加工ディジタル画像から発生してもよい。上述した中央ネットワークおよび売り点読み取り装置（本実施形態においてこの装置を、入場点またはセキュリティ点写真ＩＤ読み取り装置と考えることができる）は、本質的に、規定された直交パターンの組に対するインデックスとして働く固有番号の中央ネットワーク発生と、読み取り装置によって行われる関係するドット積演算と、中央ネットワークによって行われる同様の演算との比較とを含む前記実施形態と同じ処理を行う。この実施形態において、読み取り装置および中央ネットワークによって行われるドット積演算から発生した数が一致する場合、ネットワークは、読み取り装置に、正当すなわち交換されていない写真ＩＤ文書を示す承認を送る。

【0314】

他の実施形態において、身分証明文書１０００の写真部分１０１０を、写真ＩＤ文書に組み込まれた写真画像が上記で規定したような“配布可能信号”対応するように、ディジタル化し、処理してもよい。したがって、この場合において、前記写真は、見る人には感知できず、Ｎビット識別コードを輸送する、複合埋め込みコード信号を含む。この識別コードを、前記写真から、上述した復号化技術のいずれかを使用して、または、要求されるセキュリティのレベルに応じて万能またはカスタムコードを用いることによって抽出できることは、明らかであろう。

【0315】

前記写真に埋め込まれた情報が、前記文書において現れ読むことができる情報１０１２と相互に関係してもよく、余計な部分であってもよいことは、明らかであろう。したがって、このような文書を、写真ＩＤ文書を、パスポートまたはビザ管理点において利用可能なような走査システムにおいて置くことによって認証することができる。識別情報を抽出する万能コードを与えられるローカルコンピュータは、オペレータが、前記符号化情報と、前記文書において輸送された読むことができる情報１０１２との相関関係を確認できるように、抽出された情報をローカルコンピュータ画面に表示する。

【0316】

写真に埋め込まれた情報は、身分証明文書における他の情報と関係する必要がないことは明らかであろう。例えば、前記走査システムは、ユーザに前記写真が偽造されているかどうかの“行け”または“行くな”情報を与えるために、前記識別コードの存在を確認することのみを必要としてもよい。暗号化ディジタル通信ラインを使用するローカルコンピュータが、情報を中央証明設備に送り、その後、暗号化した“行け”または“行くな”指示を戻してもよいことも明らかであろう。

【0317】

他の実施形態において、写真に埋め込まれた識別コードを、カード運搬人の指紋のような生物測定学的データの強固なディジタル画像とし、この画像を、走査および表示後、この点における指紋認識システム（または、網膜走査、等）を用いる極めて高いセキュリティ点において、前記運搬人の実際の指紋との比較に使用してもよい。

【0318】

写真に埋め込まれた情報は、視覚的に隠れている、または、ステガノグラフィ的に埋め込まれている必要はないことは明らかであろう。例えば、識別カードに組み込まれている写真を、個々の１または２次元バーコードの画像の組み合わせとしてもよい。このバーコード情報は、前記コードから得られる情報を、例えば、前記身分証明文書に印刷された情報と比較することができるようにするための、慣例的な光学的走査技術（内部クロスチェックを含む）に属するものである。

【0319】
現在使用しているＩＤ文書の写真を、その像が写真において現れる個人に関係する情報を埋め込むことができるように処理してもよいことも考えられる。この関係において、読み手の注意は、“全体的に埋め込まれたコードを付けることができる、印刷、紙、文書、プラスチックコーティング識別カード、および他の材料”と表題のついたこの説明の前の部分に向けられ、ここでは、本テクノロジーの原理の用途に従う“信号”として扱うことができる物理的媒体の変調に対する多数のアプローチが説明されている。

【0320】
固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク化方法

図２７の図は、固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク化方法を与える本テクノロジーの態様を説明する。ある意味において、この態様は、ネットワークナビゲーションシステムであり、より広く、アドレスおよびインデックスをデータオブジェクトそれら自体に直接埋め込む、塊状に分割されたインデックス化システムである。気付くように、この態様は、ワールドワイドウェブ（WWW）において与えられるページとのホットリンクを確立することに、特に良好に適合する。所定のデータオブジェクトは、グラフィカル表現および埋め込まれたＵＲＬアドレスの双方を有効に含む。

【0321】
先の実施形態におけるように、この埋め込みを、付加されたアドレス情報がオブジェクトの重要な値に製作者および観客に関する限り影響を及ぼさないように行う。このような埋め込みの結果として、従来のWWWリンクに伴う２つのクラス（データオブジェクトおよび別個のヘッダファイル）よりも、データオブジェクトの１つのクラスのみが存在する。ホットリンクされたデータオブジェクトが１つのクラスに減る利点を上述しており、さらに以下に詳細に説明する。本テクノロジーのある実施形態において、ワールドワイドウェブを、以前から存在するネットワークを基礎とするホットリンクとして使用する。このシステムの一般的な装置は、ネットワーク化されたコンピュータや、ウェブに接続されたときの相互作用の結果を表示するコンピュータモニタである。本テクノロジーのこの実施形態は、ウェブサイト訪問者に与えられ、“グレイスケール”または“連続トーン”または“ぼかし”と、結果として生じる固有ノイズとを有する画像、ビデオ、オーディオおよび他の形態のデータオブジェクトに直接ステガノグラフィ的に埋め込まれたＵＲＬまたは他のアドレス形式情報を考察する。上述したように、基本的なステガノグラフィ的実現化を実現する種々の方法が存在し、これらのすべてを、本テクノロジーに従って用いることができる。

【0322】
図２７を特に参照して、画像、疑似連続トーングラフィックス、マルチメディアビデオおよびオーディオデータが、現在、ワールドワイドウェブにおける多くのサイト１００２、１００４の基本構成ブロックである。このようなデータを、今後、総体的に創造データファイルまたはデータオブジェクトと呼ぶ。説明する目的のため、連続トーングラフィックデータオブジェクト１００６（背景を伴うダイヤモンドリング）を図２７に示す。

【0323】
ウェブサイトツール、ウェブサイトを開発するもの１００８と、これらを閲覧するもの１０１０の双方は、種々のファイルフォーマット慣例的に処理し、これらのデータオブジェクトをパッケージ化する。しばしば、創造者側の、これらのオブジェクトによって表される製品を売り、または創造的サービスを広告する（例えば、写真家の技術およびサービスを宣伝する、８００電話番号を表示した好例の写真）希望により、これらのデータオブジェクト１００６をできるかぎり広範囲に配布することは、既に一般的である。このテクノロジーの方法を使用することにより、このようなデータオブジェクトを創造し、広める個人および組織は、ネットワークにおける彼ら自身のノード、WWWにおける彼ら自身のサイトに正しく逆上って導くアドレスリンクを埋め込むことができる。

【0324】
あるサイト１００４におけるユーザは、単に、表示されたオブジェクト１００６において、指し示し、クリックすることを必要とする。ソフトウェア１０１０は、オブジェクトをホットリンクオブジェクトとして確認する。前記ソフトウェアは、そのオブジェクトに埋め込まれたＵＲＬアドレスを読み取り、ユーザが慣例的なウェブリンクを使用しているかのように、ユーザをリンクされたウェブサイト１００２に送る。そのリンクされたサイト１００２を、オブジェクト１００６の創造者のホームページまたはネットワークノードとし、その創造者を製造者としてもよい。第1サイト１００４におけるユーザに、次に、例えば、オブジェクト１００６によって表される製品を購入するための注文用紙を与える。
【0325】
ＵＲＬアドレスまたはインデックスを埋め込まれたオブジェクト１００６（これらのオブジェクトを“ホットオブジェクト”と呼んでもよい）の創造者と、彼らの品物およびサービスを宣伝することを希望する製造者とは、彼らの創造的内容を、WWWを渡る風のなかのたんぽぽの種のように伝播させることができ、これらの種に埋め込まれているものが彼ら自身のホームページ逆上るリンクであることを知ることは明らかであろう。
【0326】
オブジェクト１００６が、グラフィックの一部として組み込まれる（図２７に示す好例の“ＨＯ”略語のような）明白なアイコン１０１２を含んでもよいことも考えられる。アイコンまたは他の微細なしるしは、オブジェクトが、埋め込まれたＵＲＬアドレス、またはソフトウェア１０１０によってアクセス可能な他の情報を輸送するホットオブジェクトであることをユーザに知らせる。
【0327】
なんらかの人間が感知しうるしるし（例えば、短い音）は、ホットオブジェクトのユーザに知らせる目的を果たすことができる。しかしながら、このようなしるしが必要ないことも考えられる。ユーザの、アドレスが埋め込まれていないデータオブジェクトにおいてクリックする試行錯誤のアプローチは、単に、ソフトウェアがＵＲＬアドレスを捜すが見つからないこと招くであろう。
【0328】
本テクノロジーのこの態様の使用における固有の自動処理は、極めて有利である。ウェブソフトウェアおよびウェブサイト開発ツールは、単に、これらにおいてリアルタイムに動作する、埋め込まれたホットリンク（ホットオブジェクト）のこの新たなクラスを認識する必要がある。慣例的なホットリンクを、ホットオブジェクトをウェブサイト貯蔵所に“アップロード”することにより、トラフィックの監視以外のことを行うためのウェブサイトプログラマを必要とすることなく、簡単に変更および付加することができる。
【0329】
本テクノロジーの上述した機能を実現する方法は、一般的に、ＵＲＬをステガノグラフィ的に画像、ビデオ、オーディオ、およびデータオブジェクトの他の形態に埋め込む基準の組を形成するステップ（１）と、この新たな形式のデータオブジェクト（ホットオブジェクト）を認識するようなウェブサイト開発ツールおよびウェブソフトウェアを設計するステップ（２）とを含み、前記ツールを、オブジェクトがユーザに与えられ、ユーザがこのようなオブジェクトを指し示し、クリックした場合、ユーザのソフトウェアが、どのようにステガノグラフィ的情報を読み取るまたは復号化し、ユーザを復号化されたＵＲＬアドレスに送るかを知るように設計する。
【0330】
ステガノグラフィ的実現化を詳細に説明した本明細書の前の部分（一般的に、図２およびそれに関係する文を参照されたい）は、本テクノロジーの実現に容易に適合する。これに関して、別の慣例的なサイト開発ツール１００８を拡張し、例えば、識別コード（例えば、ＵＲＬアドレス）を有するビットマップ化画像ファイルを、本テクノロジーに従って符号化する能力を含むようにする。本実施形態において、商用または商取引を基礎とする

ホットオブジェクトに、上述した万能コードのいずれかを使用して、ＵＲＬアドレス（または他の情報）をステガノグラフィ的に埋め込むことができる。

【0331】

ステガノグラフィ的に埋め込まれた情報を読み取るまたは復号化する技術を詳細に説明した本明細書の前の部分（一般的に、図３およびそれに関係する文を参照されたい）は、本テクノロジーの実現に容易に適合する。これに関して、別の慣例的なユーザソフトウェア１０１０を拡張し、例えば、符号化ビットマップ化ファイルを分析し、識別情報（例えば、ＵＲＬアドレス）を抽出する能力を含むようにする。

【0332】

情報をデータオブジェクトにステガノグラフィ的に埋め込む説明的な実施形態を説明したが、当業者には、多数の利用可能なステガノグラフィ的技術のいずれをも、本実施形態の機能を実行するために使用することができることが明らかであろう。

【0333】

本実施形態が、WWWのいくつかの基礎構成ブロック、すなわち、画像および音を他のウェブサイトに対するホットリンクにすることができる、直接かつ一般的な意味の機構を与えることは明らかであろう。また、このようなホットオブジェクトのプログラミングは、単に、画像およびオーディオの配布および利用度によって完全に自動化することができる。実際のウェブサイトプログラミングは必要ない。本実施形態は、非プログラマが彼らのメッセージを、単に創造的内容（ここでは、ホットオブジェクト）を形成し、配布することによって、容易に広めることができるような、WWWの商用使用を可能にする。示したように、ウェブを基礎とするホットリンクそれら自体を、より秘密のテキストを基礎とするインタフェースから、より自然な画像を基礎とするインタフェースまで取り扱うことができる。

【0334】

カプセル化ホットリンクファイルフォーマット

上述したように、一度、ホットリンクナビゲーションのステガノグラフィ的方法を理解すると、新たなファイルフォーマットおよび送信プロトコル開発として、“ヘッダを基礎とする”情報付加のより伝統的な方法が、ステガノグラフィを基礎とするシステムによって構築される基本的なアプローチを強調することができる。ステガノグラフィを基礎とするホットリンク方法をより伝統的なヘッダを基礎とする方法に拡張しはじめるある方法は、ネットワークナビゲーションシステムにおいて使用される標準的なクラスに有効になることができるファイルフォーマットの新たなクラスを規定することである。画像、オーディオ、等を越えるオブジェクトが、テキストファイル、インデックス化グラフィックファイル、コンピュータグラフィック、等を含む“ホットオブジェクト”になることができることが分かるであろう。

【0335】

カプセル化ホットリンク（ＥＨＬ）ファイルフォーマットは、簡単に、予め存在するファイルフォーマットの大きな範囲の周囲に配置された小さな殻である。ＥＨＬヘッダ情報は、何らかの種類の業界標準フォーマットにおける完全で正確なファイルが続く、ファイルの最初のNバイトのみを取り上げる。ＥＨＬスーパーヘッダは、単に、正しいファイル形式と、ＵＲＬアドレス、またはそのオブジェクトに関係する他の情報とを、ネットワークにおける他のノード、またはネットワークにおける他のデータベースに付加する。

【0336】

ＥＨＬフォーマットを、ステガノグラフィ的方法をゆっくりと置き換える（が、恐らく完全にではない）方法とすることができる。このゆっくりさは、ファイルフォーマット標準か、しばしば、形成し、実現化し、みんなが実際にしようとするのに（するとしても）極めて長くかかるというアイデアに敬意を払っている。再び、このアイデアは、その周囲に構築されたＥＨＬ様フォーマットおよびシステムが、ステガノグラフィ的方法を基礎とするシステム機構に自分でなることである。

【0337】

自己抽出ウェブオブジェクト

一般的に言って、データの３つのクラス、すなわち、番号（例えば、バイナリに符号化されたシリアルまたは識別番号）、英数字メッセージ（例えば、ＡＳＣＩＩまたは減少ビットコードにおいて符号化された人間が読むことができる名前または電話番号）またはコンピュータ命令（例えば、ＪＡＶＡまたは広範囲なＨＴＭＬ命令）をオブジェクトにステガノグラフィ的に埋め込むことができる。埋め込まれたＵＲＬおよび上述したようなものは、この第３のクラスを捜しはじめるが、可能性のより詳細な説明を助けとすることができる。

【0338】

図２７Ａに示す代表的なウェブページを考える。３つの基本的な部品、すなわち、画像（＃１－＃６）、テキストおよびレイアウトとして見てもよい。

【0339】

本願人のテクノロジーを、この情報を自己抽出オブジェクトに統合し、このオブジェクトからウェブページを再発生するのに使用することができる。

【0340】

この例によれば、図２７Ｂは、１つのＲＧＢモザイク化画像に共に適合した図２７Ａのウェブページの画像を示す。ユーザは、アドビのフォトショップソフトウェアのような存在する画像処理プログラムを手動で使用してこの操作を行うことができ、またはこの操作を、適切なソフトウェアプログラムによって自動化することができる。

【0341】

図２７Ｂのモザイクにおけるいくらかの画像タイルの間に、空き領域（斜線によって示す）がある。

【0342】

次にこのモザイク化画像を、ステガノグラフィ的に符号化し、レイアウト命令（例えば、ＨＴＭＬ）およびウェブページテキストをその中に埋め込む。前記空き領域において、損なう画像データが無いため、符号化ゲインを最大にすることができる。次に、符号化され、モザイク化された画像をＪＰＥＧ圧縮し、自己抽出ウェブページオブジェクトを形成する。

【0343】

これらのオブジェクトを、どのような他のＪＰＥＧ画像としても交換することができる。ＪＰＥＧファイルを開いた場合、適切にプログラムされたコンピュータは、埋め込まれた情報の存在を検出することができ、前記レイアウトデータおよびテキストを抽出することができる。他の情報と共に、レイアウトデータは、モザイクを形成する画像を最終的なウェブページにおいて配置すべき場所を特定する。コンピュータは、埋め込まれたＨＴＭＬ命令に従い、グラフィックス、テキスト、および他のＵＲＬへのリンクをすべて具える、オリジナルのウェブページを形成することができる。

【0344】

前記自己抽出ウェブページを慣例的なＪＰＥＧビュワーによって見た場合、自己抽出は行われない。しかしながら、ユーザは、（いくかの画像間にノイズ様“澱”を伴う）ウェブページに関係するロゴおよびアートワークを見るであろう。当業者は、これは、代表的に、完全に抽出されていない限り全体的に不明瞭に現れる、他の圧縮されたデータオブジェクト（例えば、ＰＫＺＩＰファイルおよび自己抽出テキストアーカイブ）を見ることと全く相違していることを認識するであろう。

【0345】

（上記利点を、前記ウェブページテキストおよびレイアウト命令をＪＰＥＧ圧縮モザイク化画像ファイルに関係するヘッダファイルに配置することによって、十分に達成することができる。しかしながら、このようなシステムを形成するために必要なヘッダフォーマットの業界標準は、実際的に、不可能でなくても、困難だと思われる）。

【0346】

ステガノグラフィ的に埋め込まれた画像のパレット

ＵＲＬ情報を埋め込まれたウェブ画像が一旦普及すると、このようなウェブ画像を、“パレット”に集めることができ、ユーザに高レベルナビゲーションツールとして与えることができる。ナビゲーションを、文字通りのウェブページネームにおけるクリックよりも、このような画像（例えば、異なったウェブページのロゴ）におけるクリックによって作用させる。適切にプログラムされたコンピュータは、選択された画像から埋め込まれたＵＲＬ情報を復号化することができ、要求された接続を確立することができる。

【0347】

ソフトウェアプログラムの保護および制御における本テクノロジーの可能な使用

ソフトウェアプログラムの不正使用、複製および転売は、ソフトウェア産業全体に対する収入の莫大な損失を意味する。この問題を軽減しようとする先行技術の方法は、極めて一般的であり、ここでは説明しない。説明することは、このテクノロジーの原理を、この莫大な問題にどのように関係させるかである。このテクノロジーによって与えられるツールが、場所および意図の双方において存在する対策を上回る何らかの経済的利点（考えられるすべてのこと）を有するかどうかは、全く明らかではない。

【0348】

最近の１０年またはそれ以上に渡るテクノロジーの状態は、プログラムをユーザのコンピュータにおいて機能させるために、ソフトウェアプログラムの完全なコピーを渡す必要性を作った。実際は、ＳＸは、Ｘが大きい場合、ソフトウェアプログラムの形成において使用され、その開発の全体の成果は、その全体において、ユーザがソフトウェアプログラムから価値を得るために、ユーザに渡されなければならない。幸いにも、これは一般的にコンパイルされたコードであるが、これが抽象的に見られる不確実な配布状況であることが問題である。この世の大部分の（および大部分の犯罪者の精神において無害な）プログラムの不正コピーおよび使用を、ある程度容易に行うことができる。

【0349】

この開示は、最初に、最も広い意味において経済的である（例えば、コスト比に対して回復される収入が、大部分の競争する方法のそれを越える）ことが分かるまたは分からない抽象的アプローチを提案する。このアプローチは、プラスチッククレジットおよびデビットカードの節において既に示した方法およびアプローチにおいて拡張する。“固有パターンの大きな組”を仮定することによる抽象的概念は、所定の制作物に固有であり、この制作物の所定の購入者に固有である。このパターンの組は、数千、そしてさらに数百万の完全に固有の“秘密キー”を実際に含み、暗号学用語を使用する。重要かつ明白に、これらのキーは、非決定論的であり、すなわち、これらは、ＲＳＡキーを基礎とするシステムによるように、個々のサブ１０００またはサブ２０００ビットキーから発生しない。このパターンの大きな組を、キロバイトまたはメガバイトにおいて量り、上述したように、非決定論的とする。さらに、依然として最高の抽象的レベルにおいて、これらのパターンを、標準的な技術によって暗号化し、暗号化された領域で分析することができ、ここで前記分析を、前記パターンの大きな組の小さい部分においてのみ行い、盗人志望者がマイクロプロセッサのマイクロコード命令を一歩一歩監視している最悪のシナリオにおいても、この集められた情報が、有用な情報を盗人志望者に与えないようにする。この後者の点は、以下に簡単に説明する“先天的セキュリティ”に対比して“実現化セキュリティ”になる場合、重要である。

【0350】

例えば、比較的簡単な、すでに重要視されているＲＳＡ暗号方法に対比して、この形式のキーを基礎とするシステムの特徴的な特性は何であろうか。上述したように、この考察は、商業的な面の分析を使用とするものではない。代わりに、我々は、異なった特性に焦点を置いている。主な特有の特徴は、実現化領域（実現化セキュリティ）ということになる。１つの例は、１つの低ビット数プライベートキーの単なる局所的使用または再使用が、暗号化商取引システムにおいて固有に弱いリンクであることである。［“暗号化商取引システム”は、ここで、ソフトウェアの支払済み使用の保障が、この考察において、ソフトウェアのユーザと、ユーザにプログラムを使用させる“バンク”との間の事実上暗号化

された通信を必要とする意味において考察されており、他の見方において見ると、電子金融商取引のサービスにおける暗号化である。］いわゆる安全なシステムを打ち負かしたい自称ハッカーは、方法の原始的な使用の基本的なハードワイヤ化セキュリティ（先天的セキュリティ）を決して襲わず、人間性および人間の監視の周囲に集まるこれらの方法の実現化を襲う。ここで、依然として抽象において、それ自体は非決定論的であり、実際に破棄キーに向けてより調整されている、より大きなキーベースの形成は、所定の保障システムのより歴史的なもろい実現化を“防まぬけ”しはじめる。キーの莫大な組は、これらのキーの平均保持者に理解できず、これらのキーの彼らの使用（すなわち、これらのキーの“実現化”）は、これらのキーをランダムに選択することができ、その後これらを容易に破棄することができ、これらを、“盗み聞きする人”がその盗み聞きから有用な情報をなにも得ず、特に、盗み聞きする人がキーを“解読する”ことができるまでの長い時間の内に、システムにおけるその有用さが古くなってしまうように使用することができる。

【0351】

前記抽象性を半具体的にすることにより、ソフトウェア製品をその製品の真実の購入者にのみ安全に渡す１つの可能な新たなアプローチは、以下の通りである。大規模な経済的意味において、この新たな方法は、ユーザのコンピュータネットワークと、販売会社のネットワークとの間の（しばしば、標準的暗号化をする必要がない）小規模なレートのリアルタイムディジタル接続性にもっぱら基づいている。一見して、これは、良い市場の人間の誰に対してもトラブルの匂いがし、損失収入を償おうとすることによって、重要なものを不要なものと一緒にすててしまうかもしれず、あなたは、その道（最低限の分析のすべての部分）に沿って、より正当な収入を失う。この新たな方法は、１つのソフトウェアを売る会社が、それを手に入れることを望んでいる誰かに、ユーザのネットワークに局所的な記憶装置にその機能的ソフトウェアの（速度と、送信の最少化との必要性のため）９９．８％程度を供給することを命令する。この“自由コアプログラム”を、完全に非機能的とし、最も狡猾なハッカーがそれを使用することができない、またはある意味において“逆コンパイル”できないように設計する。このプログラムの正当な活性化および使用を、単に命令サイクルカウントを基礎とすると共に、単にユーザのネットワークと会社のネットワークとの間の簡単な極めて低いオーバヘッド通信を基礎として行う。製品を使用したい客は、支払金額を会社に、多数のそうするのによい方法のいずれかによって送る。前記客に、一般的な積送り方法によって、または、一般的に保障された暗号化データチャネルを経て、彼らの“固有秘密キーの莫大な鍵”を送る。我々がこの大きな組を、画像であるかのように見ている場合、この開示の他の部分において何度も考察した雪状画像のように見える。（ここで、“署名”を、他の画像に微細に配置するよりも、画画像とする。）この画像の特別な性質は、我々が“途方もなく固有”と呼ぶものであり、多数の選択キーを含む。（“途方もない”は、“すべてのもの”が与える数と正確に等しい、１メガバイトのランダムビット値によって可能になる組み合わせの数における簡単な数学から来ており、したがって、１メガバイトは、多くの破棄選択キーを有する多くの人に対する十分な能力である、１０の２４０００００乗程度になる。）購入された存在が、文字通り、ツールの生産的使用であることを再強調することは重要である。このマーケッティングは、この生産性のその割り当てにおいて、前使用支払計画は、周知にユーザに興味を失わせ、明らかに全体的な収入を低くするため、極めて自由であることを必要とする。

【0352】

この選択キーの大きな組を、標準的な暗号化技術を使用して、それ自体暗号化する。比較的高い“実現化セキュリティ”に関する基礎は、ここで、それ自体を証明することを開始することができる。ここでユーザは、ソフトウェア製品を使いたいとする。彼らは、前記自由コアを始動させ、この自由コアプログラムは、ユーザが彼らの固有暗号化キーの大きな組をインストールしていることを見つける。前記コアプログラムは、会社ネットワークを呼び、通常のハンドシェークを行う。会社ネットワークは、キーの大きな組が真実のユーザに属することを知り、前記デビットおよびクレジットカードの節において説明したのとほとんど正確に同じ方法で、あるパターンの簡単な組において質問を送る。この質問

は、全体の小さな組のようなものであり、コアプログラムの内部の働きは、キーのすべての組を暗号解読する必要はなく、したがって、ローカルコンピュータそれ自体におけるマシンサイクル内でキーの暗号解読化されたものは存在しない。理解できるように、これは、主な開示の“画像内の署名”必要とせず、代わりに、多くの固有キーが画像である。コアプログラムは、特定のドット積を行うことによってキーに質問し、次にこれらのドット積を、確認のために会社のネットワークに送り返す。図２５と、それに伴う確認処理における代表的な詳細に関する考察とを参照されたい。一般的に暗号化された確認を送り、コアプログラムはここでそれ自体を、ある量の命令、例えば、入力されている１００００００文字をワード処理プログラムに与える命令を（他の１００００００を可能にするために送信する必要がある他の固有キーの前に）行えるようにする。この例において、購入者は、代表的に、ワードプロセッサプログラムの一人のユーザが一年の期間内に使用する命令の数を買うことができる。ここで、この製品の購入者は、このプログラムをコピーし、それを彼らの友人および親戚たちにあげる動機を持たない。

【0353】

上記すべては、２つの簡単な問題以外は良好である。第１の問題を“クローン化問題”と呼ぶことができ、第２の問題を“ビッグブラザー問題”と呼ぶことができる。この２つの問題に対する解決法は、緊密にリンクしている。後者の問題は、最終的に、純粋に社会的な問題になり、単に道具としての技術的解決法では終わらない。

【0354】

前記クローン化問題は、以下のものである。一般的に、現在一般的な著作権侵害の形式の“友人が彼らの配布ＣＤを友人に上げる”よりも、ソフトウェアのより洗練された著作権侵害に対して現れる。狡猾なハッカー“Ａ”は、その全体に“埋め込まれた”プログラムのシステム状態クローン化を行い、このクローンを他の機械にインストールした場合、この第２の機械は、実際に、同じお金に対して受ける価値を２倍にすることを知っている。このクローンをディジタル記憶装置に保持することによって、ハッカー“Ａ”は、それを再販売し、そのクローンを第１の期間が過ぎた後、再インストールする必要があるだけであり、したがって、一回の支払いに対してプログラムを無期限に使用し、すなわち、彼女は、そのクローンを彼らのハッカー友達“Ｂ”に６本パックのビールのためにあげることができる。この問題の１つのよい解決法は、再び、ユーザサイトと、会社授権ネットワークとの間の、ある程度良好に開発され、低コストのリアルタイムディジタル接続性を使用する。この偏在的接続性は、一般的に、今日存在しないが、インターネットと、ディジタルバンド幅における基本的な成長とを通じて、急速に成長している。“授権”の一部および一区分は、機能化プログラムが会社ネットワークとのハンドシェークおよび確認を日常的および不規則に行う、無視しうる通信コストランダム会計機能である。平均して、プログラムの生産性サイクルの比較的小さな量を含むサイクル中にそれを行う。結果としての平均生産性サイクルは、一般的に、全体的に授権されたプログラムのクローン化プロセスの未処理の合計コストよりもかなり低い。したがって、授権プログラムがクローン化されたとしても、その同時的なクローンの有用性は厳しく制限され、販売会社の要求する価格を支払うことは、このような短い時間周期でクローン化プロセスを繰り返すことよりも大幅にコスト効果的になる。ハッカーは、このシステムを楽しみのために破壊することができるが、利益のために破壊することは確実にできない。この配列に対する裏面は、プログラムがランダムな監査のために会社のネットワークを“呼ぶ”場合、そのプログラムにおけるそのユーザに対して割り当てられた生産性カウントが説明され、真実の支払いが受けられていない場合、会社ネットワークは、単にその確認を制止し、プログラムはもはや機能しない。我々は、ユーザが、（恐らく、彼らが本当に支払う場合、適切になり、“あなたが支払うそれと同様のなにかを行う”）明白な贈り物でない限り、友人に“これをあげる”動機を持たない場合に戻る。

【0355】

第２の問題の“ビッグブラザー”と、ユーザのネットワークおよび会社のネットワーク間の直観的に不可思議な“授権”接続とは、上述したように、すべての種類の可能な実在

および想像される解決法を有するべき、社会的かつ知覚的問題である。最高で客観的に打ち破ることができないアンチビッグブラザー解決法によっても、依然として、そうしないことを要求する中核の陰謀理論群が存在する。これを念頭において、１つの可能な解決法は、リアルタイム確認ネットワークを処理し、調整する、主に公的または非利益命令である、１つのプログラム登録をセットアップすることである。このような存在は、ユーザ客と同様に会社客を有する。例えば、ソフトウェア出版業者協会のような組織は、このような試みを導入することを選択してもよい。

【0356】

この節の結末をつけると、ここで概要を述べた方法は、高度に接続された分布されたシステム、すなわち、１９９５年中頃に存在するより偏在的で安価なインターネットを必要とすることを、再強調すべきである。未熟なディジタル通信バンド幅における成長レートも、上記システムが、最初に現れていたよりも実際的でより速くなることを主張する。（双方向ＴＶの見通しは、世界中の数百万のサイトをリンクする高速ネットワークの見込みをもたらす）。

【0357】

このテクノロジーに関係した現在の暗号化方法の使用

このテクノロジーの原理のある程度の実現化が、恐らく、現在の暗号化方法を良好に使用できることを、簡単に示すべきである。問題の１つの場合は、それによって、グラフィックアーティストおよびディジタル写真家が、かれらの写真の著作権局によるリアルタイム登録を行うシステムとしてもよい。マスタコード信号、または、そのある代表的な部分を、直接第三者の登録所に有利に送ってもよい。この場合において、写真家は、かれらのコードが安全に送信され、途中で盗まれていないことを知りたいであろう。この場合において、ある一般的な暗号化処理を用いてもよい。また、写真家またはミュージシャン、またはこのテクノロジーのなんらかのユーザは、より一般的になってきている確実な時間スタンプサービスを受けたいであろう。このようなサービスを、このテクノロジーの原理に関係して有利に使用することができる。

【0358】

不可視署名の合法または非合法の検出および除去における詳細

一般的に、所定の存在が経験的データの所定の組の中に隠れた署名を認識できる場合、同じ存在は、この署名を除去するステップを行うことができる。実際に、前の状態と後の状態との差の程度を、幸いにも、極めて大きくすることができる。ある極端において、一般的に“逆コンパイル”するのが極めて困難で、経験的データにおける承認機能を行うソフトウェアプログラムを置くことができる。一般的に、このソフトウェアの同じビットを、前記署名を（極端にすることなく）“取り除く”ことに使用することはできない。他方において、ハッカーが、わざわざ、あるデータ交換システム中で使用される“公用コード”を発見し、理解する場合、そして、ハッカーが、どのように署名を認識するかを知る場合、ハッカーが署名されたデータの所定の組を読み取り、実際に除去された署名を有するデータセットを形成するのは大きなステップではない。この後者の例において、十分に興味深く、しばしば、署名が除去されたことを暴露する統計値が存在し、これらの統計値をここでは考察しない。

【0359】

署名を除去するこれらのおよび他のこのような試みを、不正試みと呼ぶことができる。著作権法の現在および過去の展開は、一般的に、犯罪活動に属するような活動を目的としており、通常、刑罰および強制用語を伴うような言葉を決まりきった法律に配置してきた。恐らく、この署名テクノロジーのなんらかのおよびすべての弁護士は、これらの種類の著作権保護機構の不正除去を、同じ種類のａ）創造、ｂ）配布、およびｃ）使用することが、強制および刑罰を受けることを要する犯罪であること確かめることをするであろう。他方では、このテクノロジーの指摘する目的は、この開示において概要を示したステップを通じて、ソフトウェアプログラムを、署名の認識がこれらの除去に、認識プロセスにおいてこれらが見つけた信号エネルギと同じ量によって、知られた署名を反転することによ

って、容易に至ることができるように形成することができるようにすることである。この開示においてこれを指摘することによって、この署名除去動作を行うソフトウェアまたはハードウェアは、（恐らく）犯罪であるだけでなく、（恐らく）特許を受けたテクノロジーの保有者によって正しくライセンスされていない程度の違反は免れないことが明らかになる。

【0360】

署名の合法で通常の認識の場合は、簡単である。ある例において、公用署名を慎重に最低限可視に形成する（すなわち、これらの強度を慎重に高くする）ことができ、この方法において、配布する“校正刷り植字”の形成を行うことができる。“植字”および“校正刷り”は、写真業界においてかなりしばらくの間使用されており、質を落とした画像を見込みのある客に配布し、彼らがそれを評価することができるが、商業的に意味があるようには使用できないようにする。このテクノロジーの場合において、公用コードの強度の増加は、商業的価値を意識的に低下させる方法として働き、その後、題材に対する購入金額を払うことによって活性化されたハードウェアまたはソフトウェアによって、公用署名を除去する（そして可能的に、公的または私的の新たな不可視追跡コードまたは署名に置き換える）ことができる。

【0361】

監視局および監視サービス

署名の偏在的かつコスト効果的な認識は、このテクノロジーの原理を広く広めるための主な問題である。この開示のいくつかの節は、種々の方法におけるこの話題を扱う。この節は、監視ノード、監視局、および監視代理店のような存在を、本テクノロジーの原理の組織的実施の一部として形成できるというアイデアに焦点を合わせる。このような存在を動作させるために、マスタコードの知識を必要とし、その未加工の（非暗号化かつ無変換）形態における経験的データへのアクセスを要求することができる。（オリジナルの無署名経験的データへのアクセスを有することは、よりよい分析の助けとなるが、必要ではない）。

【0362】

監視局の３つの基本的な形態は、マスタコードの明白に任意に規定されたクラスから直接起こり、私的監視局、半公的および公的である。この区別は、単にマスタコードの知的を基礎としている。完全に私的な監視局の一例を、特定の基本的パターンをその配布された題材中に配置することを決め、真に狡猾な盗人が解読および除去することができることを知るが、この可能性は、経済的スケールにおいて馬鹿げたほど小さいと考える、大きな写真貯蔵社としてもよい。この貯蔵社は、高価値の広告および著作権消失状態の他の写真を受持ち、ランダムに検査し、基本的パターンを見つけるのが比較的容易なこれらを探し、その貯蔵社の社員が、それが侵害された題材かもしれないと“認め”考えた写真を検査するパートタイマーを雇う。このパートタイマーは、数時間以内にこれらの多量の侵害された可能性のある場合を巡回し、基本パターンが見つかった場合、より徹底的な分析を行い、オリジナル画像を突き止め、この開示において概略を示したような固有識別の完全な処理を行う。２つの中心的な経済的価値が、これを行う貯蔵社に対して生じ、定義によるこれらの価値は、監視サービスのコストおよび、署名処理それ自体のコストをよりもまさる。第１の価値は、彼らの客および世界が、彼らが彼らの題材に署名しており、侵害者を捕らえる能力におけるどんな統計によっても支援された監視サービスが存在することを知らせることにおけることである。これは抑止的価値であり、恐らく、結局最も大きい価値であろう。この第１の価値に対して一般的に予め必要なものは、（第１の価値を強調する）恐ろしくするための、監視努力と、その追跡記録の構築とから得られた、実際に取り戻された著作権使用料である。

【0363】

半公的監視局および公的監視局は、これらのシステムにおいて、マスタコードの知識を客によって与えられた第三者のサービスを実際に始めることができ、前記サービスが、数千および数百万の“創造的価値”を通じて捜し、コードを探索し、結果を客に報告すると

しても、大部分同じパターンに従う。ＡＳＣＡＰおよびＢＭＩは、この基本的なサービスに対する“より低い技術”のアプローチを有する。

【0364】

このテクノロジーの原理を使用する大きい調節された監視サービスは、その創造的特性供給客を２つの基本的なカテゴリーに分類し、これらは、一般的に公的領域マスタコード（と、もちろんこれら２つの混成物）を使用する。この監視サービスは、スーパーコンピュータのバンクによる高レベルパターン検査を行う、公的に利用可能な画像、ビデオ、オーディオ等の毎日の標本化（検査）を行う。雑誌広告および画像を分析のために走査し、商用チャネルの盗まれたビデオをディジタル化し、オーディオを標本化し、公的インターネットサイトをランダムにダウンロードする、等を行う。次にこれらの基本的データストリームを、その公的および私的コードの大きいバンクと、検査しているデータ題材とのパターン一致をランダムに捜す常時撹拌監視プログラムに供給する。それ自体が恐らく大きな組である小さなサブセットを、一致の可能性がある候補として合図し、これらを、正確な署名が存在することを識別し、与えられた合図された題材においてより精密に分析する試みを開始する、より精密な検査システムに供給する。恐らく、次に、小さな組が、合図された一致題材ということになり、その題材のオーナを明確に確認し、監視報告を客に送り、彼らが、彼らの題材の合法な販売であることを確認できるようにする。上記で概要を述べた私的監視サービスの同じ２つの価値は、この場合において同様に適合する。この監視サービスは、発見され、証明された侵害の場合においてフォーマットブリーとしても働き、侵害する当事者に、見つけた侵害を立証し、誇張的な著作権使用料を要求する手紙を送り、侵害する当事者が、より費用が掛かる裁判所に行く選択を回避できるようにする。

【0365】

サブリミナル登録パターンを画像および他の信号に埋め込む方法

埋め込まれた信号の読み取りの概念は、登録の概念を含む。下にあるマスタノイズ信号を知らなければならず、その関係する部分を、読み取り処理それ自体（例えば、Ｎビット識別ワードの１および０の読み取り）を始めるために、確定（登録）する必要がある。誰かが無署名信号のオリジナルまたはサムネイルへのアクセスを有する場合、この登録処理はまったく簡単である。誰かがこの信号へのアクセスを持たない場合、これは、しばしば、このテクノロジーの万能コード用途における場合となり、異なった方法をこの登録ステップを行うために用いる。定義により、“無署名”オリジナルには成らない、予め印が付けられた写真フィルムおよび紙の例は、後者の点における完全な場合である。

【0366】

多くの前の節は、この問題を種々に考察し、ある程度の解決法を与えた。明白に、“簡単な”万能コードにおける節は、所定のマスタコードか先天的に既知であるが、その正確な場所（そして、その存在または非存在）は知られていないという解決法の一実施例を考察する。この節は、極めて低いレベルの設計された信号を、極めてより大きい信号内にどのように埋め込むことができるかの特定の例を与え、ここで、この設計された信号を標準化し、検出設備または読み取り処理が、この標準化信号を、その正確な場合が分からないにもかかわらず、捜すことができるようにする。２Ｄ番号コードにおける短い節は、この基本概念を２次元、または実際に、画像および動画に拡張できることを指摘する。また、対称パターンおよびノイズパターンにおける節は、２次元の場合に対するさらに他のアプローチの概略を述べ、ここで、２次元スケールおよび回転に関係するニュアンスを、より明白に述べる。その点において、前記アイデアは、下にあるノイズパターンの正確な方向およびスケールを単に決定することではなく、同様に送信される情報、例えば、Ｎビット識別ワードに関する５つのリングを有することでもある。

【0367】

この節は、登録のために、埋め込まれたパターンを登録するサブ問題を分離することを試みる。埋め込まれたパターンが一度登録されると、我々は、この登録が、より広い要求にどのように役に立つことができるかを見ることができる。この節は、パターンを埋め込むさらに他の技術と、“サブリミナルディジタルグラティキュール”と呼ぶことができる

技術を与える。“グラティキュール”－基準、または、レチクル、または、ハッシュマークのような他の言葉は、なにかを位置決めおよび／または測定する目的に使用されるキャリブレーションマークのアイデアを伝えることに良好に使用することができる。この場合において、一種のグリッド化機能として働く低レベルパターンとして使用する。そのグリッド化機能それ自体を、１秒の万能ノイズにおけるような１ビットの情報（その不在または存在、複製化、複製不可）のキャリヤとすることができ、または、埋め込まれた信号のような他の情報の方向およびスケールを単に見つけることができ、画像またはオーディオオブジェクトそれ自体を単に適合させることができる。

【0368】

図２９および３０は、本願人のサブリミナルディジタルグラティキュールを説明する２つの関係する方法を視覚的に要約する。考察するように、図２９の方法は、図３０において概要を示した方法よりもわずかに実用的な利点を有するが、双方の方法は、解決法に収束する一連のステップへの画像の適応を見つける問題を有効に分析する。全体としての問題を、単に以下のように言うことができる。サブリミナルディジタルグラティキュールをスタンプされているかもしれない任意の画像を与えた場合、サブリミナルディジタルグラティキュールのスケール、回転、および原点（オフセット）を見つける。

【0369】

サブリミナルグラティキュールに関する開始点は、これらが何であるかを規定することである。簡単に述べると、これらは、他の画像に直接付加された、または、場合しだいで、写真フィルタまたは紙上に露出した視覚的パターンである。古典的な２重露出は、ディジタル画像化においてこの特定の概念がいくぶん拡大するとしても、悪いアナロジではない。これらのパターンは、一般的に、これらが“通常の”画像および露出と組み合わされた場合、実際に不可視（サブリミナル）になり、埋め込まれた署名による場合のように、定義によって、これらが付加された画像の広い値と干渉しないような、極めて低輝度レベルまたは露出レベルにおけるものである。

【0370】

図２９および３０は、各々、ＵＶプレーン１０００として既知の特定の周波数領域において表されるような、サブリミナルグラティキュールの２つのクラスを規定する。一般的な二次元フーリエ変換アルゴリズムは、所定の画像をそのＵＶプレーン共役に変換することができる。明確にするために、図２９および３０における描写を、特定の周波数の振幅とするが、すべての点において存在する位相および振幅を描写することは困難である。

【0371】

図２９は、４５度線に沿った各々の象限における６つの点の例１００２を示す。これらの点をＵＶプレーンの視覚的検査によって識別することは困難であるため、これらをこの図において誇張している。任意の画像の“代表的”なパワースペクトルの粗い描写１００４も示す。このパワースペクトルは、一般的に、画像が独特であるのと同じ位独特である。サブリミナルグラティキュールは、本質的にこれらの点である。この例において、２つの４５度軸の各々に沿って結合された６つの空間周波数が存在する。これら６つの周波数の振幅は、同じであっても異なってもよい（この微妙な区別については後に触れる）。一般的に言って、各々の位相は互いに異なり、他の対して４５度軸の位相を含む。図３１は、これをグラフ式に示す。この例における位相は、１００８および１０１０に、ＰＩおよび－ＰＩ間で簡単にランダムに配置されている。反映した象限はその鏡像を単にＰＩ／２ずらしたものであるため、４つの別個の象限に対して、２つの軸のみを図３１において表す。我々が、このサブリミナルグラティキュールにおける強度を大きくし、その結果を画像領域に変換した場合、図２９の説明において述べたような波状クロスハッチパターンを見るであろう。述べたように、この波状パターンは、所定の画像に付加された場合、極めて低い強度におけるものである。使用するスペクトル成分の正確な周波数および位相を格納し、標準化する。これらは、登録設備および読み取りプロセスが求め、測定する、“スペクトル署名”になる。

【0372】

簡単に、図３０は、この同じ一般的なテーマにおける変形例を有する。図３０は、スペクトル周波数が、４５度軸に沿った点よりも、同心リングの簡単な列になる、グラティキュールの異なったクラスを示す。図３２は、疑似ランダム位相プロファイルを半周期に沿った関数として示す（周期の他の半分は、最初の半分の位相からＰＩ／２ずれている）。これらは簡単な例であり、これらの同心リングの位相プロファイルおよび半径の設計において可能な、広範囲に種々の変形例が存在する。この形式のサブリミナルグラティキュールの変形は、図２９の波状グラティキュールによるような“パターン”が少なく、雪状画像のようなランダムな様子が多い。

【0373】

双方の形式のグラティキュールの背後のアイデアは、以下の通りである。固有パターンを、それが付加されている画像から常に視覚的に区別されるが、パターンの高速な位置決めを容易にする特定の特性と、パターンが一般的に位置決めされた場合、その正確な場所および方向を、ある大家レベルの精密さで見つけることができるような精度特性とを有する画像に埋め込む。上記に対する結果は、パターンが、平均して、それを付加する代表的な画像と僅かにしか干渉せず、パターンの可視度に対して最大のエネルギを有する、パターンを設計することである。

【0374】

全体的なプロセスがどのように働くかのすべての要約を進むと、図２９のグラティキュール形式は、サブリミナルグラティキュールの回転軸を最初に位置決めすることによって始まり、次にグラティキュールのスケールを位置決めし、次に原点またはオフセットを決定する、画像処理調査を容易にする。ここで、最後のステップは、軸が２つの４５度軸のいずれであるかを、位相を決定することによって確認する。したがって、画像が大きく混乱していても、正確な決定を行うことができる。第１のステップおよび第２のステップを、位相および振幅と対比して、パワースペクトルデータのみを使用して行うことができる。次に、位相および振幅信号を使用して、正確な回転角およびスケールの調査の“細かい調整”を行うことができる。図３０のグラティキュールは、上記最初の２つのステップを切り替え、最初にスケール、次に回転を見つけ、原点の正確な決定を続ける。当業者は、これらの顕著なパラメータを２つの軸に沿って決定することが、画像を完全に登録するために十分であることを、認識するであろう。“工業的最適化の挑戦”は、パターンの固有さおよび輝度をこれらの可視度に対して最大にし、登録における精度のある特定のレベルに到達することにおける計算オーバヘッドを最小にすることである。写真フィルムおよび紙を露出する場合において、明らかに、追加の工業的挑戦は、まず第１に、フィルムおよび紙上に露出したパターンを得る経済的ステップの概略であり、この挑戦は、前の節において指摘されている。

【0375】

上記で規定した問題および解決法は、登録の目的のための登録を意図するものである。グラティキュールが実際に見つかっているかどうかにおけるある種の評価判断の形成によって形成される記載はないことに注意されたい。明らかに、上記ステップを、実際にその内部にグラティキュールを持たない画像に用いることができ、このとき測定は、単にノイズを追跡する。共感が、これらのパターンの形式に対する“検出しきい値”を設定する仕事を割り当てられたエンジニア、または、パターンを捜し、確認する必要がある画像および周囲の状態の途方もなく広い範囲の中の誰かに広がる必要がある。〔反語的に、これは、純粋に万能な一秒のノイズを前の節において置いたことであり、この単一の信号を単に検出する、または検出しないを越えていく、すなわち、追加の情報プレーンを追加することがなぜ適切なのかである。〕こういう事情は、サブリミナルグラティキュールの、この開示の他の部分において説明した登録された埋め込まれた署名との結合において、ある本当の美人が現れることである。明確に、ノイズを追跡することができるアイデアに敬意を払い、一度“志願者登録”が見つかると、次の論理的ステップは、例えば、６４ビット万能コード署名の、読み取り処理を行うことである。他の例として、我々は、６４ビット識別ワードの４４ビットを、登録されたユーザのインデックス、こういう言い方を許しても

らえるならばシリアル番号として割り当てることを想像することができる。残りの２０ビットを、このように得られた４４ビット識別コードにおける、暗号化技術においてよく知られている、ハッシュコードとして確保する。したがって、一挙に、２０ビットが、“はい、私は登録された画像を持っています”または“いいえ、私は持っていません”の答えとして働く。より重要に、ひょっとすると、これは、どのような自動化識別システムにおいても、“誤った肯定”のレベルを正確に規定することにおいて最高に柔軟にすることができるシステムを考慮する。しきい値を基礎とする検出は、常に、最終的に任意の決定に基づく過剰な状態および状況のなすがままになるであろう。いつの日もＮのコイン投げを与えてくれ。

【0376】

点に戻ると、これらのグラティキュールパターンを、最初に、画像に付加するか、フィルム上に露出しなければならない。好例のプログラムは、任意のサイズのディジタル画像において読み取り、特定したグラティキュールをこのディジタル画像に付加し、出力画像を発生する。フィルムの場合において、グラティキュールパターンをフィルム上に、本来の画像の露出中または後に、物理的に露出する。これらの方法のすべては、これらをどのように行うかにおいて、広い変形例を有する。

【0377】

サブリミナルグラティキュールの探索および登録は、より興味深く、必要とされるプロセスである。この節は、最初に、このプロセスの要素を説明し、図３７の一般化したフローチャートにおいて終わる。

【0378】

図３３は、図２９における形式のグラティキュールに対する登録プロセスの第１の主要な“探索”ステップを示す。疑わしい画像（または、疑わしい写真の走査）を、最初に、既知の２Ｄ　ＦＦＴルーチンを使用して、そのフーリエ表現に変換する。入力画像は、図３６の左上のもののように見える。図３３は、続く処理が回転問題に完全に対処するとしても、画像およびグラティキュールが回転されていない場合を概念的に表す。疑わしい画像を変換した後、変換のパワースペクトルを計算し、２つの自乗した係数の和の平方根とする。３×３ブラーフィルタのような軽いローパスフィルタ処理を結果として得られたパワースペクトルデータに行い、後の探索ステップが途方もなく細かい間隔のステップを必要としなくなるようにすることも、良いアイデアである。次に、０ないし９０度の候補回転角（または、半径において０ないしＰＩ／２）を進める。何らかの角度に沿って、２つの結果として生じるベクトルを計算し、第１のベクトルは、各々の象限における原点から放射する４本のラインに沿った所定の角度におけるパワースペクトル値の単純な足し算である。第２のベクトルは、第１のベクトルの移動平均である。次に、規格化パワープロファイルを、１０２２および１０２４に示すように計算し、その違いは、一方のプロットが、サブリミナルグラティキュールと整列しない角度に沿っており、他方のプロットは整列している。規格化は、第１のベクトルが結果として得られるベクトルの分子であり、第２のベクトルが分母であることを規定する。図３３の１０２２および１０２４において分かるように、ピークの列（図示した“５”の代わりに“６”にすべき）は、角度がその本来の方向に沿って整列する場合に現れる。これらのピークの検出を、あるしきい値を前記規格化値に設定し、これらの合計を半径ライン全体に沿って積分することによって行うことができる。０ないし９０度のプロット１０２６を図３３の下部に示し、これは、角度４５度が最大エネルギを含むことを示す。実際に、この信号は、しばしば、この下部の図に示すよりもかなり低く、最高値を“見つかった回転角”として選択する代わりに、単に、少数の最高の候補角を見つけ、これらの候補を、登録を決定するプロセスの次の段階に提出することができる。前述のことが単に既知の信号検出計画であり、最終的に形成または借用することができるこのような多数の計画が存在する技術の当業者によって、理解することができる。第１段階のプロセスの簡単な必要なことは、候補回転角をいくつかに減らすことであり、次に、より精密な探索が引き継ぐことができる。

【0379】

図３４は、パワースペクトル領域における同様の形式の全体的な探索の概要を本質的に述べる。ここで代わりに、我々は、回転角よりも、最初に同心リングの全体的なスケールに対して、小さいスケールから大きいスケールまで進むことよって、探索する。１０３２に示すグラフは、１０２２および１０２４と同じ規格化ベクトルであるが、ここでは、ベクトル値を半円に沿った角度の関数としてプロットした。前記移動平均分母を、依然として、接線方向よりも半径方向において計算する必要がある。プロット１０４０を生じることによって理解できるように、規格化信号における同様の“ピーク化”は、走査された円が、グラティキュール円と一致する場合に生じる。次にスケールを、下部のプロットにおいて、同心リングの既知の特徴（すなわち、これらの半径）を１０４０におけるプロファイルと一致させることによって見つけることができる。

【0380】

図３５は、図２９における形式のサブリミナルグラティキュールを登録することにおける第２の主要なステップを示す。一度、我々が図３３の方法によっていくつかの回転候補を見つけると、次に、我々は、１０２２および１０２４の形式の候補角のプロットを取り、本発明者が、これらのベクトルにおけるフィルタ処理動作に適合する“スケール化カーネル”と呼ぶことを行う。スケール化カーネルは、この場合におけるカーネルが、１０４２および１０４４の上部におけるｘのラインとして表される既知の周波数の非調和関係であり、これらの周波数のスケールが、ある要求される１００％におけるスケールの２５％ないし４００％のようなある予め決められた範囲に広がることに関係する。整合フィルタ演算は、単に、結果として生じるスケール化周波数の乗算された値と、これらのプロットの片側とを加算する。当業者は、この演算の、極めて良く知られている整合フィルタ演算との類似性を認識するであろう。整合フィルタ演算の結果として得られるプロットは、いくらか図３５の下部における１０４６のように見える。前記第１ステップからの各々の候補角は、それ自身のこのようなプロットを発生し、この時点においてこれらのプロットの最高値が我々の候補スケールになる。図３０の形式のグラティキュールと同様に、同様の“スケール化カーネル”整合フィルタ演算を、図３４のプロット１０４０において行う。これは、一般的に、１つの候補スケール係数を与える。次に、図３２の格納された位相プロット１０１２、１０１４および１０１６を使用して、より慣例的な整合フィルタ演算を、（カーネルとして）これらの格納されたプロットと、前に見つかったスケールにおける半周期に沿って測定された位相プロファイルとの間に用いる。

【0381】

図２９の形式のグラティキュールの登録の最後のステップは、グラティキュールの既知の（スペクトルまたは空間）プロファイルと、疑わしい画像との間の、普通の種々の整合フィルタ演算を行うことである。回転、スケールおよび方向が、前のステップによって分かっていることから、この整合フィルタ演算は簡単である。正確で精密な前のステップが、処理において設計仕様を越えていない場合、簡単な小規模の探索を、スケールおよび回転の２つのパラメータについて小さい領域において行うことができ、行われた整合フィルタ演算と、見つかった最高値とは、“細かく調節された”スケールおよび回転を決定する。この方法において、スケールおよび回転を、疑わしい画像それ自体のノイズおよびクロストークによって設定された程度内で見つけることができる。同様に、一度、図３０の形式のグラティキュールのスケールおよび回転が見つかると、簡単な整合フィルタ演算は、この登録プロセスを完了することができ、同様に、“細かい調節”を適用することができる。

【0382】

図２９、図３６の形式のグラティキュールの使用の変形に進むことは、計算に関して不経済な二次元ＦＦＴ（高速フーリエ変換）を行う必要なく、サブリミナルグラティキュールを見つける可能性を与える。計算オーバヘッドが大きな問題である状況において、探索問題を、一連の一次元ステップに減少させることができる。図３６は、これをどのように行うかを明白に示す。左上におけるこの図は、図２９の形式のグラティキュールが埋め込まれた任意の画像である。０度から始め、例えば５度ずつ進み、１８０度で終わることに

よって、図示した列に沿ったグレイ値を単純に加算し、結果として得られる列－積分走査１０５８を形成することができる。この図の右上、１０５２は、これを行う多くの角度の１つを示す。次にこの列－積分走査を、計算に関してあまり不経済でない一次元ＦＦＴを使用して、そのフーリエ表現に変換する。次にこれを、振幅または“パワー”プロット（これら２つは異なる）に変え、図３３における１０２２および１０２４と同様の規格化ベクトルバージョンを形成する。ここでの違いは、角度がグラティキュールの正しい角度に近づくにつれ、１０２４のようなプロットにおいて、表示ピークがゆっくりと現れ始めるが、これらは、我々は一般的に我々の回転において僅かに外れていることから、一般的に、所定のスケールに要求されるよりも高い周波数において現れることである。ピーク信号を最大にする角度を見つけることが残っており、したがって、正しい角度においてズームインする。一度、正しい回転が見つかると、スケール化カーネル整合フィルタ処理を行うことができ、すべて上述した慣例的な整合フィルタ処理を続ける。再び、図３６の“ショートカット”の１つのアイデアは、図２９における形式のグラティキュールを使用することにおける計算オーバヘッドを大幅に減少させることである。本発明者は、たとえ実現されるとしても、図３６のこの方法を習慣のため減少させておらず、正確にどの位計算に関して節約できるかにおけるデータを現在持たない。これらの試みは、方法の用途を特定した発展の一部である。

【0383】

図３７は、主要なプロセスステップの順序における、図２９の形式のグラティキュールの周囲を回転する方法を簡単に要約する。

【0384】

他の変形実施形態において、グラティキュールエネルギは、空間周波数領域において４５度に関係しない。代わりに、このエネルギは、より広く空間的に分布する。図２９Ａは、あるこのような分布を示す。軸の近傍および原点の近傍の周波数は、画像エネルギが最も集中すると思われる場所であるため、一般的に無効になる。

【0385】

疑わしい画像におけるこのエネルギの検出は、再び、上述したような技術を頼る。しかしながら、最初に軸を確認し、次に回転を確認し、次にスケールを確認する代わりに、すべてを暴力的試みにおいて決定する、より包括的な整合手順を行う。当業者は、フーリエ－メリン変換が、このようなパターン整合プログラムにおける使用に好適であることを認識するであろう。

【0386】

前述の原理は、例えば、写真複製キオスクにおける用途を得る。このような装置は、代表的に、客が与えたオリジナル（例えば、写真プリントまたはフィルム）を光電子検出器に結像するレンズと、感光乳剤基板（再び、印画紙またはフィルム）を前記検出器によって得られた画像データに従って、露出し、現像するプリント書き込み装置とを含む。このような装置の詳細は、当業者には既知であり、ここでは考察しない。

【0387】

このようなシステムにおいて、メモリは前記検出器からのデータを格納し、プロセッサ（例えば、支持部品と関係するペンティアムマイクロプロセッサ）を使用し、メモリデータを処理し、それにステガノグラフィ的に埋め込まれた著作権データの存在を検出することができる。このようなデータが検出された場合、プリント書き込みを中断する。

【0388】

オリジナル画像の軸から外れた手動の回転によるシステムの失敗を回避するために、前記プロセッサは、上述した技術を望ましく実現化し、スケール、回転および原点のオフセット因子にもかかわらず、オリジナルの自動登録を行う。もし望むなら、ディジタル信号処理ボードを使用し、メイン（例えば、ペンティアム）プロセッサによるＦＦＴ処理のある程度を取り除くことができる。回転した／スケール化した画像を登録した後、どのようなステガノグラフィ的に埋め込まれた著作権情報の検出も簡単であり、機械が写真家の著作権の侵害において使用さないことを確実にする。

【0389】
開示した技術は、本願人の好むステガノグラフィ的符号化方法の使用を行ったが、その原理を、より広く適用でき、画像の自動登録を行うべき多くの場合において使用することができる。
【0390】
ビデオデータストリームが高速一方向モデムとして効率的に働く、ビデオに埋め込まれた信号の使用
以前の節において概要を述べた万能コード化システムの使用によって、そして、簡単な方法でフレーム毎に変化するマスタ雪状フレームの使用によって、簡単な受信機を、マスタ雪状フレームにおける変化の予めの知識を有し、したがって、フレーム毎（または、ＭＰＥＧビデオにおけるとしてもよい場合のようにＩフレーム毎）に変化するＮビットメッセージワードを読み取ることができるように設計することができる。この方法において、動画シーケンスを、一方向モデムのような、高速一方向情報チャネルとして使用することができる。例えば、ステガノグラフィ的に埋め込まれ、Ｎビットメッセージの送信を行うＮ本の走査ラインを有するビデオデータのフレームを考える。フレーム（Ｎ）において４８４走査ラインが存在し、フレームが一秒に３０回変化する場合、１４．４キロボードモデムに匹敵する容量を有する情報チャネルが達成される。
【0391】
実際において、フレーム当たりＮビットの超過において十分なデータレートが通常達成され、ＩＳＤＮ回路の送信レートに近い送信レートになる。
【0392】
無線通信における詐欺防止
セルラ電話産業において、サービスの盗難により、毎年１億ドルの収入が損失する。いくつかのサービスは、セルラ電話の物理的盗難によって損失するが、より有害な脅迫がセルラ電話ハッカーによってもたらされる。セルラ電話ハッカーは、種々の電子装置を用い、許可されたセルラ電話によって発生された識別信号を模倣する。（これらの信号は、時々、許可信号、識別番号、署名データ、等と呼ばれる。）しばしば、ハッカーは、これらの信号を、許可されたセルラ電話加入者を盗み聞きし、セルサイトと交換されたデータを記録することによって学習する。このデータの巧妙な使用によって、ハッカーは、許可された加入者を真似ることができ、キャリヤを騙して非合法な通話を完成することができる。
【0393】
先行技術において、識別信号を音声信号から分離する。最も一般的に、これらは、時間的に分離され、例えば、通話開始時にバーストにおいて送信される。音声データは、証明動作がこの識別データにおいて行われた後にのみ、チャネルを通過する（識別データを、一般的に、送信中に送られるデータパケットにも含める）。他のアプローチは、識別を、例えば、音声データに割り当てられたバンド以外のスペクトルサブバンドにおいて、スペクトル的に分離することである。
【0394】
他の詐欺防止計画も用いられている。あるクラスの技術は、セルラ電話のＲＦ信号の特徴を監視し、源を発する電話を識別する。他のクラスの技術は、ハンドシェークプロトコルを使用し、セルラ電話によって返されたデータのいくらかが、それに送られるランダムデータに用いられるアルゴリズム（例えば、ハッシュ化）を基礎とする。
【0395】
前述のアプローチの組み合わせも、時々用いられる。
【0396】
米国特許明細書第5,465,387 号、第5,454,027 号、第5,420,910 号、第5,448,760 号、第5,335,278 号、第5,345,595 号、第5,144,649 号、第5,204,902 号、第5,153,919 号および第5,388,212 号は、種々のセルラ電話システムと、そこで使用される詐欺防止技術とを詳述している。これらの特許の開示は、参照によって取り入れられる。

【0397】
詐欺防止システムの洗練度が増すにつれて、セルラ電話ハッカーの洗練度も増している。最終的に、ハッカーは、彼らが、全ての先行技術システムが同じ弱点、すなわち、識別が音声データ以外のセルラ電話送信のある属性を基礎としていることに対して脆いことを認識しているため、より優勢である。この属性は、音声データから分離されていることから、このようなシステムは、これらの音声を、詐欺防止システムを破るのに必要な属性を有する複合電子信号に、電子的に“でっち上げる”盗人に対して常に影響を受けやすい。
【0398】
この欠点を克服するために、本テクノロジーのこの態様の好適実施形態は、音声信号を識別データと共にステガノグラフィ的に符号化し、結果として、“帯域内”周波信号（時間およびスペクトルの双方において帯域内）を生じる。このアプローチは、キャリヤがユーザの音声信号を監視し、そこから識別データを複合かすることを可能にする。
【0399】
本テクノロジーのあるこのような形態において、先行技術において使用されている識別データのいくらかまたはすべて（例えば、通話開始時に送信されるデータ）を、同様にユーザの音声信号に繰り返しステガノグラフィ的に符号化する。したがってキャリヤは、音声データに伴う識別データを通話開始時に送られる識別データと周期的または非周期的に検査し、これらの一致を保証する。これらが一致しない場合、この通話を、ハックされていると認め、通話を中断するような改善のためのステップを行うことができる。
【0400】
本テクノロジーの他の形態において、いくつかの可能なメッセージのランダムに選択された１つを、電話加入者の音声に繰り返しステガノグラフィ的に符号化する。通話開始時にセルラキャリヤに送られたインデックスは、期待されるメッセージを認識する。電話加入者の音声からセルラキャリヤによってステガノグラフィ的に復号化されたメッセージが期待されたものと一致しない場合、この通話を不正として認識する。
【0401】
本テクノロジーのこの態様の好適な形態において、ステガノグラフィ的符号化は、疑似ランダムデータ信号を頼り、メッセージまたは識別データを、電話加入者のディジタル化された音声信号に重ねられた低レベルノイズ状信号に変換する。この疑似ランダムデータ信号は、（符号化に関して）電話加入者の電話と、（復号化に関して）セルラキャリヤとの双方に対して知られている、または知られうる。多くのこのような実施形態は、電話およびキャリヤの双方に対して知られている基準の種を蒔かれた決定論的疑似ランダム数発生器を頼っている。簡単な実施形態において、この種を、あるセルから次のセルまで一定（例えば、電話ＩＤ番号）のままにすることができる。より複雑な実施形態において、疑似一回パッドシステムを使用することができ、新たな種を各々のセッション（すなわち、通話）に対して使用する。混成システムにおいて、電話およびセルラキャリヤの各々は、基準ノイズキー（例えば、１００００ビット）を有し、そこから電話は、ランダムに選択されたオフセットにおいて開始する５０ビットのようなビットの領域を選択し、各々がこの抜粋を種として使用し、符号化のための疑似ランダムデータを発生する。通話開始中に電話からキャリヤに送られたデータ（例えばオフセット）は、キャリヤに、復号化に使用する同じ疑似ランダムデータを再構成させる。さらに他の改善を、基本的技術を暗号通信の技術から借用し、これらをこの開示において詳述したステガノグラフィ的に埋め込まれた信号に用いることによって得ることができる。
【0402】
疑似ランダムデータストリームによるステガノグラフィ的符号化／復号化に関する本願人が好む技術の詳細は、本明細書の以前の部分においてより特に詳述されているが、このテクノロジーは、このような技術との使用に限定されない。
【0403】
読み手が、セルラ通信技術に精通しているとする。したがって、この分野における先行技術から既知の詳細を、ここでは考察しない。

【0404】
図３８を参照すると、説明的なセルラシステムは、電話２０１０と、セルラサイト２０１２と、中央局２０１４とを含む。
【0405】
概念的に、電話を、マイクロフォン２０１６と、Ａ／Ｄコンバータ２０１８と、データフォーマッタ２０２０と、変調器２０２２と、ＲＦセクション２０２４と、アンテナ２０２６と、復調器２０２８と、データアンフォーマッタ２０３０と、Ｄ／Ａコンバータ２０３２と、スピーカ２０３４を含むものとして見ることができる。
【0406】
動作において、電話加入者の音声は、マイクロフォン２０１６によって拾われ、Ａ／Ｄコンバータ２０１８によってディジタル形態に変換される。データフォーマッタ２０２０は、ディジタル化された音声を、パケット形態にし、同期化および制御ビットを付加する。変調器２０２２は、このディジタルデータストリームを、位相および／または振幅が変調されているデータに従って変化するアナログ信号に変換する。ＲＦセクション２０２４は、一般的に、この時間変化する信号を、１つ以上の中間周波数に変え、最終的にＵＨＦ送信周波数に変える。ＲＦセクションは、その後、それを増幅し、結果として得られる信号を、セルサイト２０１２に放送するためにアンテナ２０２６に供給する。
【0407】
このプロセスは、受信時に逆に働く。セルサイトからの放送は、アンテナ２０２６によって受信される。ＲＦセクション２０２４は、受信された信号を増幅し、復調のための異なった周波数に変える。復調器２０２８は、ＲＦセクションから供給された信号の振幅および／または位相変化を処理し、それに対応するディジタルデータストリームを発生する。データアンフォーマッタ２０３０は、関係する同期化／制御データから音声データを分離し、この音声データをアナログ形態に変換するためにＤ／Ａコンバータに渡す。Ｄ／Ａコンバータからの出力は、スピーカ２０３４を駆動し、これを通じて電話加入者は、他の関係者の音声を聞く。
【0408】
セルサイト２０１２は、複数の電話２０２０からの放送を受信し、受信されたデータを中央局２０１４に中継する。同様に、セルサイト２０１２は、中央局から出たデータを受信し、同じものを電話に放送する。
【0409】
中央局２０１４は、セル認証、切り替え、およびセルハンドオフを含む種々の動作を行う。
【0410】
（いくつかのシステムにおいて、セルサイトおよび中央局間の機能区分が、上記で概略を述べたものと異なる。実際は、いくつかのシステムにおいて、この機能のすべては、１つのサイトにおいて与えられる）。
【0411】
本テクノロジーのこの態様の好例の実施形態において、各々の電話２０１０は、ステガノグラフィ的エンコーダ２０３６を追加して含む。同様に、各々のセルサイトは、ステガノグラフィ的デコーダ２０３８を含む。前記エンコーダは、動作し、補助データ信号を電話加入者の音声を表す信号の中に隠す。前記デコーダは、逆の機能を行い、補助データ信号を符号化された音声信号から区別する。この補助信号は、セルの合法性を確認するために働く。
【0412】
好例のステガノグラフィ的エンコーダ２０３６を図３９に示す。
【0413】
示したエンコーダ２０３６は、ディジタル化音声データ、補助データ、および疑似ランダムノイズ（ＰＲＮ）データにおいて動作する。ディジタル化音声データをポート２０４０に用い、例えば、Ａ／Ｄコンバータ２０１８から与える。ディジタル化音声データは、

８ビット標本を具えてもよい。補助データをポート２０４２に用い、補助データは、本テクノロジーの１つの形態において、電話２０１０を固有に識別するバイナリデータのストリームを具えてもよい。（補助データは、通話開始時にセルサイトと習慣的に交換される種類の管理上のデータを追加で含んでもよい。）疑似ランダムデータ信号をポート２０４４において用い、例えば、値“－１”および“１”間でランダムに起こる信号とすることができる。（ますますセルラ電話は、拡張されたスペクトルを受けられる回路網を取り入れており、この疑似ランダムノイズ信号および、このテクノロジーの他の態様は、しばしば、セルラユニットの基本的動作に既に用いられている回路網を“背負う”または共有することができる）。

【0414】

説明に便利なため、エンコーダ２０３６に印加される３つのデータ信号すべてを共通のレートでクロック動作させるが、これは実際には必要ない。

【0415】

動作において、補助データおよびＰＲＮデータストリームを論理回路２０４６の2つの入力部に印加する。回路２０４６の出力信号は、以下の表に従って、－１および＋１の間で切り替わる。

【0416】

【表1】

補助	ＰＲＮ	出力
0	－１	１
0	１	－１
１	－１	－１
１	１	１

【0417】

（補助データ信号を０および１の代わりに－１および１間の切り替わりとして考える場合、回路２０４６が１ビット倍率器として動作することが分かる）。

【0418】

したがって、ゲート２０４６からの出力信号は、瞬時の値が補助データおよびＰＲＮデータの対応する値に従ってランダムに変化するバイポーラデータストリームである。しかしながら、その中に符号化された補助データを有する。対応するＰＲＮデータを知っている場合、補助データを抽出することができる。

【0419】

ゲート２０４６からのノイズ様信号を、スケーラ回路２０４８の入力部に印加する。このスケーラ回路は、この入力信号を、ゲイン制御回路２０５０によって設定された係数によってスケール化（例えば、倍加）する。示した実施形態において、この係数は、０ないし１５間で変動しうる。したがって、スケーラ回路２０４８からの出力信号を、補助およびＰＲＮデータと、スケーラ係数とに従って、各々のクロック周期で変化する５ビットデ

ータワード（４ビットに加え符号ビット）として表すことができる。このスケーラ回路からの出力信号を、“スケール化ノイズデータ”として考えることができる（しかし、再び、ＰＲＮデータを与えた場合、そこから補助データを取り戻すことができる“ノイズ”である）。

【0420】

このスケール化ノイズデータを、加算器２０５１によってディジタル化音声信号に加算し、符号化出力信号（例えば、標本ごとに２値的に加算された）を発生する。この出力信号は、ディジタル化音声データおよび補助データの双方を表す複合信号である。

【0421】

ゲイン制御回路２０５０は、ディジタル化音声データへのその加算が、アナログ形態に変換され、電話加入者によって聞かれた場合、音声データを顕著に劣化させないように、加算されるスケール化ノイズデータの振幅を制御する。このゲイン制御回路は、種々の方法において動作することができる。

【0422】

１つは、対数的スケール化機能である。したがって、例えば、１０進法値０、１または２を有する音声データ標本を、１または０のスケール係数に対応させてもよく、２００以上の値を有する音声データ標本が、１５のスケール係数に対応してもよい。一般的に言って、スケール係数および音声データ値は、平方根関係によって対応する。すなわち、音声データの値における４倍の増加は、これらに関係するスケール化係数の値における２倍の増加に対応する。他のスケール化係数は、音声信号の平均パワーから得られるため、線形である。

【0423】

（スケール化係数としてのゼロに対する挿話的な参照は、例えば、ディジタル化音声信号標本に、本質的に情報内容が無い場合を言及する）。

【0424】

瞬時のスケール化係数が１つの音声信号データ標本を基礎とするよりも満足てことは、スケール化係数がいくつかの標本の力学を基礎とすることである。すなわち、急速に変化しているディジタル化音声データのストリームは、ゆっくりと変化しているディジタル化音声データのストリームよりも、比較的、補助データを隠す恐れがある。したがって、ゲイン制御回路２０５０を、スケール化係数の設定において、音声データの１次、または好適には２次またはより高次の導関数に応じさせることができる。

【0425】

依然として他の実施形態において、ゲイン制御ブロック２０５０およびスケーラ２０４８を、完全に省略してもよい。

【0426】

（当業者は、前記システムにおける“レールエラー”の可能性を認識するであろう。例えば、ディジタル化音声データが８ビット標本から成り、これらの標本が０から２５５（１０進法）までの全体の範囲に及ぶ場合、入力信号へのスケール化ノイズの加算、または入力信号からのスケール化ノイズの減算は、８ビットによって表すことができない出力信号（例えば、－２または２５７）を発生するかもしれない。この状況を修正する多数のよく理解された技術が存在し、これらのいくつかは順行的であり、これらのいくつかは反動的である。これらの既知の技術に共通して、ディジタル化音声データが０－４または２４１－２５５における値を持たず、それによって、スケール化ノイズ信号との結合を安全に許可することを指定し、そうしなければレールエラーを生じるディジタル化音声標本を検出し、適応的に修正する対策を含んでいる）。

【0427】

電話２０１０に戻って、エンコーダ２０３６は、上記で詳述したようなエンコーダ２０３６を、Ａ／Ｄコンバータ２０１８とデータフォーマッタ２０２０との間に好適に置き、それによって、補助データを伴うすべての音声送信をステガノグラフィ的に符号化させる。さらに、電話の動作を制御する回路網またはソフトウェアを、補助データが繰り返し符

号化されるように配置する。すなわち、補助データの全てのビットが符号化された場合、ポインタが輪になって戻り、エンコーダ２０３６に印加すべき補助データを新たにする。（補助データを、参照を簡単にするためにＲＡＭメモリにおける既知のアドレスにおいて格納してもよい）。

【0428】

示した実施形態における補助データは、音声データのレートの８分の１のレートにおいて送信されることを認識されるであろう。すなわち、音声データの８ビット標本ごとに、補助データの１つの信号ビットに対応するスケール化ノイズデータが送られる。したがって、音声標本が４８００標本／秒のレートにおいて送られる場合、補助データを４８００ビット／秒のレートにおいて送ることができる。補助データを８ビット記号で構成した場合、補助データを６００記号／秒のレートにおいて輸送することができる。補助データが均一な６０記号のストリングから成る場合、各秒の音声は、補助データを１０回輸送する。（極めてより高い補助データレートを、制限された記号コード（例えば、５または6ビットコード）、ハフマン符号化、等のような、より効率的な符号化技術の力を借りることによって達成することができる。）この補助データの高度に冗長的な送信は、使用すべきスケール化ノイズデータのより小さい振幅を可能にし、依然として、無線送信に関する比較的ノイズの多い環境においても確実な復号化を保証するのに十分な信号対ノイズヘッドルームを与える。

【0429】

ここで図４０に戻ると、各々のセルサイト２０１２は、ステガノグラフィ的デコーダ２０３８を具え、これによって、電話２０１０によって放送された複合データ信号を分析し、そこから補助データおよびディジタル化音声データを識別し、分離することができる。（このデコーダは、好適には、フォーマット化されていないデータ（すなわち、パケットオーバヘッド、制御および管理上のビットを除去されたデータ、これを説明を簡単にするために図示しない）において動作する。

【0430】

未知の音声信号からの未知の埋め込まれた信号（すなわち、埋め込まれた補助信号）の復号化は、複合データ信号の統計的分析のある形態によって、最適に行われる。上述したこの技術を、ここでも等しく用いることができる。例えば、エントロピを基礎とするアプローチを利用することができる。この場合において、補助データを（８ビット毎の代わりに）４８０ビット毎に繰り返す。上記のように、エントロピを基礎とする復号化プロセスは、複合信号の４８０番目毎の標本を同様に取り扱う。特に、このプロセスは、複合データ信号の、１番目、４８１番目、９６１番目、等の標本を符号化すると共に、ＰＲＮデータに加算することから始まる。（すなわち、疎らなＰＲＮデータの組、すなわちオリジナルのＰＲＮの組を、すべての、しかし４８０番目毎のゼロにした基準に加算する。）次に、これらの点の周囲の結果として生じる信号（すなわち、４８０番目毎の標本を変更された複合データ信号）を計算する。

【0431】

次に上記ステップを繰り返し、この時、１番目、４８１番目、９６１番目、等の複合データ標本から、これらに対応するＰＲＮデータを減算する。

【0432】

これらの２つの演算の一方は、符号化プロセスを反対に作用（例えば、取り消す）し、結果として生じる信号のエントロピを減少させ、他方は増加させる。疎らなＰＲＮデータを複合データに加算することがそのエントロピを減少させる場合、このデータは、オリジナルの音声信号からより以前に減算されているに違いない。これは、補助データ信号の対応するビットが、これらの標本が符号化された場合、“０”になることを示す。（論理回路４６の補助データ入力における“０”は、その出力基準として、対応するＰＲＮ基準の反転したものを発生させ、結果として、対応するＰＲＮ基準の音声信号からの減算が生じる）。

【0433】

相違して、複合データから疎らなＰＲＮデータを減算することがそのエントロピを減少させる場合、復号化プロセスはより以前にこの信号を加算したに違いない。これは、補助データビットの値が、標本１、４８１、９６１等が符号化された場合、“１”になることを示す。

【0434】

エントロピが、（ａ）複合データへのＰＲＮデータの疎らな組の加算、または、（ｂ）複合データからのＰＲＮデータの疎らな組の減算によって、より低くなった場合に注意することによって、補助データの最初のビットが（ａ）“０”であるか、または（ｂ）“１”であるかを決定することができる。（実際の用途において、種々の歪み現象の存在において、複合信号を十分に劣化させ、疎らなＰＲＮデータの加算も減算も、実際にエントロピを減少させないようにしてもよい。代わりに、双方の演算は、エントロピを増加させるであろう。この場合において、“適切な”演算を、どの演算がエントロピを少なく増加させるかを観察することによって、識別することができる）。

【0435】

次に、上記演算を、２番の標本から始めた複合信号の間隔をおいた標本（すなわち、２，４８２，９６２，．．．）のグループに行う。結果として生じる信号のエントロピは、補助データ信号の第２ビットが“０”または“１”のいずれであるかを示す。コードワードのすべての４８０ビットが識別されるまで、複合信号における間隔を置いた標本の４７８のグループを同様に続ける。

【0436】

上述したように、複合データ信号とＰＲＮデータとの相互関係を、統計的検出技術として使用することができる。このような演算は、現在の文脈において、その符号化表現が、先天的に、少なくとも大きい部分において、調査され、知られている補助データから、容易になる。（本テクノロジーの１つの形態において、補助データは、セルラシステムは既に受信し、記録している、通話開始時に交換される認証データを基礎としており、他の形態（以下に詳述する）において、補助データは、予め決められたメッセージを具える。）したがって、前記問題を軽減することができ、（未知の信号全体を捜すよりも）期待される信号が存在するかどうかを決定することができる。さらに、データフォーマッタ２０２０は、複合データを既知の長さのフレームに分解する。（既知のＧＳＭ実現化において、音声データを、各々が１１４データビットを輸送するタイムスロットにおいて送る。）補助データを必要に応じて拡張することによって、補助データの各々の繰り返しを、例えば、このようなデータのフレームの開始において開始させることができる。これは、１１４の可能なビットアラインメント毎の１１３を無視することができるため、相関関係決定を非常に簡単にする（先天的に既知の補助データが無いとしても、復号化を助ける）。

【0437】

再び、この無線詐欺検出は、ノイズ中の既知の信号を検出することの現在ありふれた問題を提出し、前に考察したアプローチをここで等しく用いることができる。

【0438】

補助信号の場所が先天的に既知である（またはより正確に、上述したように、いくつかの別個の場所のうちの１つになることが既知である）場合、前記整合フィルタアプローチを、しばしば、疎らなＰＲＮデータの組と、これらに対応する複合信号の平均を除いた引用との簡単なベクトルドット積に減少させることができる。（ＰＲＮデータを疎らにする必要はなく、以前に言及した英国特許公開明細書第２１９６１６７号におけるような、接近するバーストに達してもよいことに注意されたい。ここで、メッセージにおける所定のビットは、それに関係する接近したＰＲＮ値を有する。）このようなプロセスは、ＰＲＮデータの４８０の疎らな組のすべてを進み、対応するドット積演算を行う。このドット積が正の場合、補助データ信号の対応するビットは“１”であり、ドット積が負の場合、補助データ信号の対応するビットは“０”である。構成した複合信号内の補助データ信号のいくつかのアラインメントが可能である場合、この手順を各々の候補アラインメントにおいて繰り返し、最高相関関係を生じるものを真として選択する。（一度、正しいアライン

メントが補助データ信号の１つのビットに対して決定されると、他のすべてのビットのアラインメントを、そこから決定することができる。ひょっとすると“同期化”としてより知られている“アラインメント”を、主として、音声信号それ自体をロックオンして追跡し、セルラユニットの基本的な機能を考慮する全く同じ機構によって達成することができる。

【0439】

セキュリティの考え

今説明した実施形態のセキュリティは、大きな部分において、ＰＲＮデータのセキュリティおよび／または補助データのセキュリティに依存する。以下の考察において、これらのデータのセキュリティを保証する多くの技術のいくつかを考察する。

【0440】

第１の実施形態において、各々の電話２０１０に、その電話に固有の長いノイズキーを与える。このキーを、例えば、ＲＯＭに格納された高度に固有の１００００ビットストリングとしてもよい。（大部分の用途において、キーは、使用してもよいこれよりも実際的に短い）。

【0441】

中央局２０１４は、すべての許可された電話に関するこのようなキーデータを格納する保障ディスク２０５２へのアクセスを有する。（このディスクを、中央局それ自体から離してもよい）。

【0442】

電話を使用する度に、このノイズキーからの５０ビットを識別し、決定論的疑似ランダム数発生器に対する種として使用する。このＰＲＮ発生器によって発生されたデータは、その通話に関するＰＲＮデータとして働く。

【0443】

この５０ビット種を、例えば、通話のために電話を使用する度に０ないし９９５０のオフセットアドレスを発生する、電話におけるランダム数発生器によって決定することができる。このオフセットアドレスにおいて開始するノイズキーの５５ビットを、前記種として使用する。

【0444】

通話開始中、このオフセットアドレスを、電話によって、セルサイト２０１２を経て中央局２０１４に送信する。ここで、中央局におけるコンピュータは、オフセットアドレスを使用し、その電話に関するノイズキーのその複製をインデックス化する。それによって、中央局は、電話において識別されるのと同じ５０ビット種を識別する。次に、中央局２０１４は、これらの５０ビットをセルサイト２０１２に中継し、ここで、電話におけるものと類似した決定論的ノイズ発生器が、この５０ビットキーに対応するＰＲＮシーケンスを発生し、その検出器２０３８に供給する。

【0445】

前述のプロセスによって、ＰＲＮの同じシーケンスが、電話およびセルサイトの双方において発生する。したがって、電話によって音声データにおいて符号化された補助信号を、セルサイトに安全に送信することができ、セルサイトによって正確に復号化することができる。この補助データが期待される補助データ（例えば、通話開始時に送信されたデータ）と一致しない場合、この通話を不正としてフラグを立て、適切な矯正動作を起こす。

【0446】

通話開始情報の無線送信を盗み聞いている人は、電話によってセルサイトに送信されるランダムに発生されたオフセットアドレスのみを傍受できることが、認識されるであろう。このデータは、単独では、通話を盗むことにおいて役に立たない。ハッカーが、中央局からセルサイトに与えられた信号にアクセスしたとしても、このデータも本質的に役に立たず、与えられるすべては５０ビット種である。この種は、近い各々の通話に関して異なる（９９５０の通話ごとに１つのみ繰り返す）ことから、ハッカーには無益である。

【0447】

関係するシステムにおいて、１００００ビットノイズキーの全体を、種として使用することができる。通話開始中に電話によってランダムに発生されたオフセットアドレスを使用し、その種から結果として得られるＰＲＮデータにおいて、そのセッションに使用すべきＰＲＮデータを開始することを示す。（１秒あたり４８００音声標本として、４８００ＲＰＮデータが１秒あたり必要であり、すなわち１７万程度のＲＰＮデータが１時間あたり必要である。したがって、この変形実施形態におけるオフセットアドレスは、上述したオフセットアドレスよりもはるかに大きくなると思われる）。

【0448】

この変形実施形態において、復号化に使用されるＲＰＮデータを、好適には、中央局において１００００ビット種から発生し、セルサイトに中継する。（セキュリティ上の理由のため、１００００ビットノイズキーは、中央局のセキュリティを離れるべきではない）。

【0449】

上記システムの変形において、この逆にするよりも、オフセットアドレスを、中央局によって、またはセルサイトにおいて発生し、通話開始中に電話に中継することができる。

【0450】

他の実施形態において、電話１０２０に、中央局における保障ディスク２０５２において格納された種のリストと一致する、１回種のリストを与えてもよい。新たな通話を始めるために電話を使用する度に、このリストにおける次の種を使用する。この配置によって、種に関する交換にデータは必要なく、電話およびキャリヤの各々は、独立に、どの種を使用し、現在のセッションのための疑似ランダムデータシーケンスを発生するかを知る。

【0451】

このような実施形態において、キャリヤは、電話がその種のリストをほぼ使い果たす時を決定することができ、代わりのリストを（例えば、電話に対して臨時に与えられる管理データの一部として）送信することができる。セキュリティを増すために、キャリヤは、電話を手動再プログラミングに戻し、この変動しやすい情報の無線送信を回避することを要求してもよい。代わりに、代わりの種リストを、種々の既知の技術のいずれかを使用して、無線送信のために暗号化することができる。

【0452】

実施形態の第２のクラスにおいて、セキュリティは、ＰＲＮデータのセキュリティからだけでなく、そこから符号化された補助メッセージデータのセキュリティからも派生する。あるこのようなシステムは、２５６の可能なメッセージからランダムに選択された１つの送信に頼っている。

【0453】

この実施形態において、電話におけるＲＯＭは、２５６の異なったメッセージを格納する（各々のメッセージを、例えば、長さにおいて１２８ビットとしてもよい）。通話を開始するために電話を操作した場合、電話は、１ないし２５６の番号をランダムに発生し、この番号は、これらの格納されたメッセージに対するインデックスとして働く。このインデックスを、通話開始中にセルサイトに送信し、中央局に、同じ２５６のメッセージを含む保障ディスクにおける一致データベースからの期待されるメッセージを識別させる。（各々の電話は、メッセージの異なった集合を有する。）（代わりに、キャリヤは、通話開始中にインデックス番号をランダムに選択し、それを電話に送信し、そのセッション中に使用すべきメッセージを識別してもよい。）保障システムに企てられる攻撃が現実に数学的のみである理論的に純粋な世界において、これらの付加的なセキュリティのレイヤの多くは、過剰に見えるかもしれない。（メッセージ自体を異ならせるような、これらのセキュリティの付加的レイヤの追加は、単に、実際の公的に機能する保障システムの設計者が、このテクノロジーの中心的原理の数学的セキュリティを危うくするかもしれない、ある実現化経済に直面するであろうことを認める）。

【0454】

その後、その通話中に電話によって送信されたすべての音声データを、インデックス化

メッセージと共にステガノグラフィ的に符号化する。セルサイトは、期待されるメッセージの存在に関して、電話から受けたデータを検査する。そのメッセージがない場合、または、異なったメッセージが代わりに復号化された場合、その通話を、不正であるとしてフラグを立て、矯正動作を起こす。

【0455】

この第２の実施形態において、符号化および復号化に使用されるＰＲＮデータを、望むだけ簡単にも複雑にもすることができる。簡単なシステムは、各々のセルに対して、同じＰＲＮデータを使用する。このようなデータを、例えば、電話に対して固有であり、中央局によっても知られている固定されたデータ（例えば、電話識別子）を種とする決定論的ＰＲＮ発生器によって発生してもよく、または、万能ノイズシーケンスを使用することができる（すなわち、同じノイズシーケンスを、すべての電話に対して使用することができる）。または、疑似ランダムデータを、（例えば、例えば目的電話番号、等を識別する、通話開始中に送信されるデータを基礎とする）通話毎に変化するデータを種とする決定論的ＰＲＮ発生器によって発生することができる。いくつかの実施形態は、疑似ランダム数発生器に、前の通話からのデータの種を蒔いてもよい（このデータは，電話およびキャリヤに対して必然的に既知であるが、盗人には未知であると思われるため）。

【0456】

もちろん、前記２つのアプローチからの要素を、種々の方法において結合することができ、他の特徴を付加することができる。前記実施形態は、単に好例であり、使用することができる無数のアプローチのカタログを作りはじめはしない。一般的に言って、電話およびセルサイト／中央局の双方によって必然的に知られるまたは知られうるどのようなデータも、補助メッセージデータ、またはそれを符号化するＰＲＮデータのいずれかに対する基礎として使用することができる。

【0457】

本テクノロジーのこの態様の好適実施例は、電話加入者のディジタル化音声の持続時間の間中、補助データを各々ランダムに符号化するため、補助データを、受信されたオーディオのどのような短い標本からも復号化することができる。本テクノロジーのこの態様の好適な形態において、キャリヤは、ステガノグラフィ的に符号化された補助データを、（例えば、１０秒ごと、またはランダムな間隔において）繰り返し検査し、期待される属性を持ちつづけていることを保証する。

【0458】

前記考察は、セルラ電話からの送信をステガノグラフィ的に符号化することに焦点をおいていたが、同様に、セルラ電話への送信をステガノグラフィ的に符号化できることが認識されるであろう。このような配置は、例えば、管理データ（すなわち、非音声データ）のキャリヤから個々の電話への輸送において適切である。この管理データを、例えば、目標とされるセルラ電話（またはすべてのセルラ電話）を中央局から再プログラムする、（上述したオンタイムパッドシステムを用いるシステムに関する）種リストを更新する、良く知らない局所領域に固有のデータを“徘徊する”セルラ電話に知らせる、等に使用することができる。

【0459】

いくつかの実施形態において、キャリヤは、セルラ電話に、そのセルラ電話がそのセッションの残りの間にキャリヤへの送信において使用する種をステガノグラフィ的に送信してもよい。

【0460】

前記考察は、ベースバンドディジタル化音声データのステガノグラフィ的符号化に焦点を置いていたが、当業者は、中間周波数信号（アナログまたはディジタル）を、同様に、本テクノロジーの原理に従ってステガノグラフィ的に符号化できることを認識するであろう。ポストベースバンド信号の利点は、これらの中間周波数信号のバンド幅がベースバンド信号と比べて比較的広く、より多くの補助信号をその中に符号化することができ、または、一定の量の補助信号を送信中により頻繁に繰り返すことができることである。（中間

信号のステガノグラフィ的符号化を用いた場合、符号化によって導入される変動が、パケットフォーマットによって支持されるエラー訂正設備を考慮して、管理データの確実な送信に影響するほど大きくならないように注意すべきである）。

【0461】

当業者は、補助データそれ自体を、既知の方法において配置し、デコーダ３８によるエラー検出、またはエラー検出能力を援助させることができることを認識するであろう。興味を持った読み手は、このような技術を詳述する多くの容易に利用可能な教科書のうちの１つ、例えば、ローラバウ，エラー符号化クックブック，マグローヒル，１９９６を参照されたい。

【0462】

本テクノロジーのこの態様の好適実施形態を、パケット化データを使用するセルラシステムの文脈において説明したが、他の無線システムは、このような便利に構成されたデータを用いない。構成化を同期化の援助として使用できないシステムにおいて、同期化を、本願人の先行出願に詳述するような技術を使用して、複合データ信号内で達成することができる。あるクラスのこのような技術において、補助データそれ自体が、その同期化を容易にする特徴を有する。他のクラスの技術において、補助データは、アラインメントおよび検出を容易にするように設計された１つ以上の埋め込まれたキャリヤパターンを変調する。

【0463】

以前示したように、本テクノロジーの原理は、上記で詳述したステガノグラフィ的符号化の特別な形態との使用に限定されない。実際は、既知の、または後に発明されるどのようなステガノグラフィ的符号化技術も、上記で詳述した方法において、セルラ（または、他の無線、例えば、ＰＣＳ）通信システムのセキュリティまたは機能を増すために使用することができる。同様に、これらの原理は、無線電話に限定されず、どのような無線通信にも、この形式の“バンド内”チャネルを与えることできる。

【0464】

本願人のテクノロジーを実現するシステムは、専用のハードウェア回路素子を具えることができるが、より一般的に、関係するＲＡＭおよびＲＯＭメモリを有する適切にプログラムされたマイクロプロセッサ（例えば、電話２０１０、セルサイト２０１２、および中央局２０１４の各々におけるこのようなシステム）を具えることもできることを認識されるであろう。

【0465】

ビットセルによる符号化

前記考察は、個々の画素の値の増加または減少に焦点を置き、疑似ランダム信号に結合された補助データ信号の符号化を反映する。以下の考察は、補助データを、疑似ランダム化無しで、ここでビットセルと呼ぶ、画素のパターン化されたグループによって符号化する変形実施形態を詳述する。

【0466】

図４１Ａおよび４１Ｂを参照して、２つの説明的な２×２ビットセルを示す。図４１Ａを使用して補助データの“０”ビットを表し、図４１Ｂを使用して“１”ビットを表す。動作において、下にある画像の画素を、ビットセルの＋／－値に従って引き上げまたは引き下ろし、これらの２つのビット値の１つを表す。（以下に詳述するように、画像の所定の画素または領域を引く大きさを、多くの因子の関するとすることができる。特徴パターンを規定することが、引く合図である。）復号化において、符号化画素の相対的バイアスを（上述した技術を使用して）調査し、符号化画像の各々の対応する領域に関して、２つのパターンのどちらを表すかを識別する。

【0467】

この実施形態において、補助データを明白にランダム化しないが、ビットセルパターンを、上述したように、“設計された”キャリヤ信号とみなしてもよいことが認識されるであろう。

【0468】
この“設計された”情報キャリヤの、前記実施形態の疑似ランダムノイズとの交換は、ビットセルパターン化が、フーリエ空間におけるそれ自体を明らかにするという利点をもたらす。したがって、ビットセルパターン化は、上述したサブリミナルディジタルグラティキュールのように働くことができ、疑わしい画像の登録を助け、スケール／回転エラーを除去する。ビットセルのサイズと、それにおけるパターンとを変化させることによって、空間変換領域におけるそれによって与えられるエネルギの場所を変更することができ、代表的な画像エネルギからのインピーダンスを最適化し、検出を容易にする。
【0469】
（前記考察は、補助データを、ＰＲＮ信号によるランダム化無しで、直接符号化することを考えたが、他の実施形態にいて、もちろん、ランダム化を使用することができる）。
【0470】
概念的により適合した署名
既に説明した実施の形態のうちのいくつかにおいて、署名エネルギの大きさを領域間に基づいて適合させて、画像中で目に見えなく（又は、音声中で聞こえにくく）する。以下の説明中、出願人は、画像中の隠蔽署名エネルギの問題、これにより課された分離の問題、及びこれら問題の各々の解決を、更に特別に考察する。署名プロセスの目的は、単なる動作を越えて、所定のユーザ／クリエータによる固定された「見えやすさ／許容しうるしきい値」のある形態に適合しながら嵌め込まれた署名の「数字の検出可能さ」を最大にすることである。
【0471】
この目的に対して設計するためのサービスに当たり、以下の３軸パラメータスペースを考え、この場合、これら軸のうちの二つを半軸（正のみ）とし、第３の軸を、全軸（正負）とする。軸のこのセットは、ユークリッド３次元の通常の８個のスペースのうち二つを規定する。事象を洗練するとともに「分離する価値がある」パラメータが（拡張された局所的な見えやすさのマトリックス」のような）シーン上に現れると、それらは、（一般的には）それら自体の半軸を規定するとともに３次元を越える以下の例に拡張することができる。
【0472】
署名設計目的は、上記スペースの座標に基づく局所的なバンプに「ゲイン」を最適に割り当て始め、その間、基本的には、実際の用途において動作を迅速にする必要があることを留意しておく。先ず、３軸を以下のようにする。二つの半軸をｘ及びｙとし、全軸をｚとする。
【0473】
ｘ軸は、単一バンプの輝度を表す。基本的な概念は、僅かなエネルギを搾りだして、ぼやかした領域に対して領域を明るくすることである。重要なことは、真の「サイコ－リニア－装置独立」輝度値（画素ＤＮ）が現れると、輝度値が他の作動軸（例えば、Ｃ＊ ｘｙ）に結合する場合には、この軸は不必要となる。この際、これは、ここまで現在の疑似線形輝度符号化の副次的な最適化が原因となっている。
【0474】
ｙ軸は、バンプそれ自体が見つける範囲内の隣接する「局所的な隠蔽ポテンシャル」である。基本的な概念は、眼が平坦領域のような微妙な変化を検出することができるので、平坦領域が低隠蔽ポテンシャルを有することである。非常にスムーズな長いラインの「破損及び切断」も幾分目に見えるので、長いライン及び長いエッジは、隠蔽ポテンシャルが低くなる傾向にあり、短いライン及びエッチング情報及びそのモザイクは、隠蔽ポテンシャルが高くなる傾向にある。長い及び短いこれらの概念は、処理時間の問題及びパラメータのような慎重な定量化に必要な処理手段の問題に直接結びつく。ｙ軸の動作モデルの展開は、必然的に一部の気難しい芸術家の経験論に対して一部の理論を伴う。ｙ軸部分を寄せ集めるに従ってより知識が増えるので、それらは分裂して、価値がある場合にはそれら自体の独立した軸となる。

【0475】
ｚ軸は、（後に説明するように）「ゲインを伴う又はゲインに反する」軸であり、他の二つが半軸であるのに対してこれは全軸である。基本的な概念は、所定の入力バンプが、その位置で「１」又は「０」に符号化したいかに対して予め存在するバイアスを有し、それはある程度、用いられる読出しアルゴリズムの関数となり、その（バイアスの）大きさは、ｙ軸の「隠蔽ポテンシャル」に幾分相関し、それを、当該バンプにどの程度の大きさのトウィーク値を割り当てるかを決定する際に変数として、好適に用いることができる。相伴う基本概念は、バンプが既に友達である（、すなわち、その近隣に対するバイアスが所望のΔ値となる傾向にある）場合、それを大幅に変えてはいけない。その既に自然な状態は、局所的な画像値を大幅に、場合によっては全く変えることなく、復号化に必要なデータエネルギーを提供する。それに対して、バンプが最初に敵である（すなわち、その近隣に対するバイアスが、符号化によって課されるべきと考えられるΔ値から離れる傾向にある）場合、それを大幅に変えなさい。この後者の動作は、ポイントが目に見えにくくなる傾向がある（非常に局所的なぼんやりした動作）その近隣に対するこのポイントの偏位を減少させるとともに、復号化の際に検出可能な追加のエネルギを供給する。これら二つの場合、ここでは、これら二つの場合を、「ゲインを伴う」及び「ゲインに反する」と称する。
【0476】
既に説明したような問題の一般的な概念は、数年間十分である必要がある。明らかに、クロミナンスの問題を加えることは、規定をやや拡張し、より大きな見えやすさに対する署名バングとなり、圧縮の問題に適用される人間の見えやすさの調査を、正反対の理由がない場合にはこの区域に等しく適用することができる。ここでは、典型的な用途で用いることができる原理を説明する。
【0477】
スピードのために、局所的な隠蔽ポテンシャルを、画素の３×３隣接に基づいてのみ計算することができる。スピードの問題以外には、より大きいものを支持するデータ又は固有の理論も存在しない。設計の問題を要約すると、ｙ軸の見えやすさ、輝度をこれに結合する方法、及び些細な友達／敵の非対称である。ガイド原理は、平坦区域を単に零とし、従来の純粋な最大又は最小領域を「１．０」すなわち最大値とし、「局所的なライン」、「円滑な傾斜」、「鞍型ポイント」を有するとともにこれらの間のどこかで何も拡散しないことである。
【0478】
典型的な用途は、６個の基本パラメータ、１）輝度、２）局所的な平均の差、３）（ゲインに伴う又はゲインに反する）非対称因子、４）最小線形因子（平坦対ライン対最大の粗い試み）、５）ビット平面バイアス因子、６）全体ゲイン（ユーザの単一トップレベルゲインノブ）を用いる。
【0479】
輝度パラメータと、局所的な平均からの差のパラメータは、線形的であり、その使用は、本明細書以外で指定される。
【0480】
非対称因子は、２より上の差軸の「ゲインに反する」側に適用される単一スカラーである。
【0481】
最小線形因子は、明らかに粗いが、それを３×３隣接セッティングでさえあるサービスを行うべきである。この概念は、真の２Ｄ最小及び最大が３×３隣接の中央画素を横断する４ラインの各々に沿って非常にかきまわされ、視覚的なライン又はエッジが四つの線形プロファイル少なくとも一つをのばす傾向にある。〔四つの線形プロファイルをそれぞれ長さ方向に３画素とする。すなわち、左上画素－中央－右下；真上－中央－真下；右上－中央－左下；右側－中央－左側〕行方向の三つの画素に適用されるようなエントロピのマトリックスを選択し、四つの全ての線形プロファイル上でこれを実行し、その後、「ｙ軸」

として用いるべき最大パラメータに対して最小値を選択する。

【0482】

ビット平面バイアス因子は、２面、すなわち以前に空の面及び次に空の面を有する面白いものである。前者の場合、単に、署名されていない画像を「読み出す」とともに全てのバイアスが全てのビット平面に対して外れる場所を見て、全体的に所望のメッセージに反して進行するビット平面の「全体ゲイン」を簡単に引き上げるとともに、他のもののみ、すなわちそのゲインより僅かに低いものを取り除く。後に空の場合、以前に空のビットプレーンバイアス及びここでリストした他の５パラメータを有する全署名プロセスを実行し、例えば、画像をプリントした後に走査するラインスクリーンの大きなＪＰＥＧ圧縮ＡＮＤモデルの「ゲスタルト歪み」を介した署名画像を実行し、その画像を読み出すとともに、どのビットプレーンが混乱している又はエラー状態にあるかを発見し、ビットプレーンバイアスを適切に補強し、プ櫓接続を再び実行する。拡充プロセスを行う良好なデータを有する場合、このステップを１回実行するだけでよく、すなわち、バン－チッタタイズ(Wan-Cittertize)プロセスを容易に行うことができる（トウィークに適用したある緩衝係数でプロセスを繰り返すために曖昧に参照する）。

【0483】

最後に、全体ゲインが存在する。その目的は、この単一変数を、所望の場合には少しでも興味のあるユーザが調整することができるトップレベル「強度ノブ」（より典型的には、図面的なユーザインタフェースのスライダー又は他の制御）にすることである。非常に興味があるユーザは、進行したメニューを下げて、他の５個の変数上で経験的に処理する。

【0484】

目に見える透かし

ある用途において、目に見える徴候を画像に供給して、それがステガノグラフィックに符号化されたデータを含むことを表すことが望ましい。一例において、この徴候を、画像の１コーナに付与される僅かに眼に見えるロゴ（時々「透かし」と称される。）とすることができる。これは、画像が「スマートな」画像であり、像に加えてデータを搬送することを示す。電球は、一つの適切なロゴである。

【0485】

他の用途

開示した技術に対する一つの用途は、Adobe's Photoshop softwareのような画像処理ソフトウェアを用いるためのマーキング／デコーディング「プラグイン」のようなものである。一旦、このような画像のマーキングが広がると、このようなソフトウェアのユーザは、はめ込まれたデータを画像から復号化するとともに、公衆登録所を調べて、画像の所有権者を識別する。ある例では、保護は、適切なロイヤリティの支払いがユーザの画像の使用に対する所有権者に行われる管路として作用することができる（図示した例において、登録所は、データベースに結合され、ＷＷＷを介してアクセス可能なインターネットのサーバとなる。データベースは、画像それ自体が符号化される情報コードによって示された、カタログを作成した画像の詳細な情報（例えば、所有権者の名前、住所、電話番号や、画像に行うことができる種々のタイプの使用に対する料金表）を含む。画像を復号化する者は、このように集めたコードを用いて所有権者を質問し、所望の場合には、画像の所有権者に著作権のロイヤリティを電子的に支払う）。

【0486】

他の用途は、スマートなビジネスカードであり、この場合、ビジネスカードに、目立たない、機械で読出し可能なはめ込まれたコンタクトデータを有する写真を設ける（同一機能を、データをはめ込むカードの表面マイクロトポロジーを変化させることによって達成する）。

【0487】

更に別の期待できる用途は、内容規格におけるものである。テレビジョン信号、インターネット上の画像、及び他の内容源（音声、画像、ビデオ等）は、外的に関連するよりは

内容それ自体に実際にはめ込まれた「適正」（すなわち、セックス、暴力、子供に対する適正等に対する等級）を表すデータを有することができる。テレビジョン受像機、インターネットサーフィングソフトウエア等は、（例えば、全体的なコード復号化の使用による）このような適正の等級を明確に理解することができ、適切な動作（例えば、画像又はビデオを見ることを許可しない、又は音源を再生しない。）を行うことができる。

【0488】

これまで説明したうちの簡単な例において、はめ込まれたデータは、一つ以上の「フラグ」ビットを有することができる。あるフラグは、「子供に対する不適切」を示す（他のものを、例えば「この画像はコピーライトされています」又は「この画像は公衆領域です」とすることができる。）。このようなフラグビットを、はめ込まれたメッセージとは別個の制御ビットのフィールド内にある、すなわち、それ自体をメッセージとすることができる。これらフラグビットの状態を検査することにより、デコーダのソフトウェアは、画像の種々の特性のユーザを迅速に知らせることができる。

【0489】

（制御ビットを、－サブリミナルグラティクルに対して既知の－画像の既知の位置で符号化することができ、はめ込まれたデータ（例えば、その長さ、そのタイプ等）のフォーマットを示すことができる。このように、これら制御ビットは、従来のファイルヘッダで時々搬送されるデータに類似しているが、この場合、これらを、ファイルに対して考察する代わりに、画像内にはめ込む）。

【0490】

製品のマーキングの分野は、一般に、普通のバーコード及び全体の製品コードによって十分利用されている。しかしながら、所定の用途において、このようなバーコードは、（例えば、エステティックを考慮する場合、又は、セキュリティに関する場合）不所望である。このような用途において、出願人の技術は、無害のキャリア（例えば、製品に関する写真）を介して、又は製品の表面のマイクロトポロジー又はその上のラベルを符号化することにより、製品にマークすることができる。

【0491】

ステファノグラフィに暗号化及び／又はディジタル署名技術を有効に組み合わせて安全性を増大させる－非常に多くて詳細に説明できない－用途がある。

【0492】

医療記録は、証明が重要な分野に現れる。－フィルムに基づく記録又は文書のマイクロトポロジーに適用されるステファノグラフィ原理を用いて、不正に対する保護を行うことができる。

【0493】

多くの産業、例えば自動車及び旅客機は、重要な部分をマークする札を信頼する。しかしながら、このような札は容易に取り除かれ、時々偽造される。安全性がより望まれる用途において、会社の部分をステファノグラフィクにマークして、目立たない識別／証明札を提供することができる。

【0494】

本明細書で見た種々の用途において、相違するメッセージを、画像の相違する領域によって関連的に搬送することができる（例えば、画像の相違する領域は、相違するインターネットＵＲＬを提供することができ、フォトコラージュの相違する領域は相違する写真家を識別することができる。）。他のメディア（例えば、音声）についても同様である。

【0495】

あるソフトウェアビジョナリーは、データの塊がデータ波形を辿るときのデータを観察して、他のデータの塊に相互作用させる。このようなときにおいて、このような塊が強固であり、正当にそれ自体を識別する必要がある。ここでも、ステガノグラフィの技術により、保証の信頼性を増すことができる。

【0496】

最後に、メッセージ変換コード－ステファノグラフィックに符号化されたメッセージが

、内在するステファノグラフィックなコードパターンを実際に変える回帰的なシステム－は、新たなレベルの洗練及び安全を提供する。このようなメッセージ変換コードは、時間変化要素が安全性を高めるのに重要なプラスチックキャッシュカードのような用途に非常に好適である。

【0497】

また、使用者が、既に説明したようなステファノグラフィックな符号化の特定の形態を好む場合、本明細書に開示したものとは別の用途を、他のステファノグラフィックなマーキング技術を用いて広く実現することができ、その多くは従来既知である。また、同様に、本明細書は、画像に対してこの技術の用途を強調したが、その原理を、一般に、音声、物理的なメディアのこのような情報、又は情報の他の任意のキャリアのはめ込みにも同様に適用することができる。

【0498】

多数の実施の形態及びその変形を参照してこの技術の原理を説明したが、この技術を、この原理を逸脱することなく装置中で変形することができる。したがって、以下の請求の範囲及びその等価物の範囲内で全ての実施の形態を、本発明として請求する。

【図面の簡単な説明】

【0499】

【図1】２つの軸において分離された１次元ディジタル信号の簡単かつ古典的な線図である。

【図2】“微細の”認証信号を他の信号上に埋め込む処理の、ステップの詳細な記述による全体的な概観である。

【図3】オリジナルの疑わしいコピーをどのように検証するかについての漸次の説明である。

【図4】本発明の他の実施例による検証情報によってフィルムを前露光する装置の線図である。

【図5】本発明の“ブラックボックス”実施例の図表である。

【図6】図５の実施例のブロック図である。

【図7】異なったコードワードを有するが同じノイズデータを有する入力データの連続する組を符号化するのに適合した図６の実施例の変形例を示す。

【図8】特有のコード番号を有するビデオテープ製造の各々のフレームを符号化するのに適合した図６の実施例の変形例を示す。

【図9】Ａ～Ｃは、本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。

【図10】標準ノイズコードの検出において使用される集積回路を示す。

【図11】図１０の実施例において使用することができる標準ノイズコードを検出する処理の流れを示す。

【図12】本発明の他の実施例による複数の検出器を使用する実施例である。

【図13】疑似ランダムノイズフレームを画像から発生する実施形態を示す。

【図14】信号の統計を復号化の援助においてどのように使用できるかを示す。

【図15】どのように署名信号を使用し、予測される歪み（例えば、ＭＰＥＧ）の視点におけるその堅牢さを増すかを示す。

【図16】ファイルについての情報をヘッダおよびファイル自体において詳述する実施形態を示す。

【図17】ファイルについての情報をヘッダおよびファイル自体において詳述する実施形態を示す。

【図18】回転対象パターンを使用する実施形態に関する詳細を示す。

【図19】回転対象パターンを使用する実施形態に関する詳細を示す。

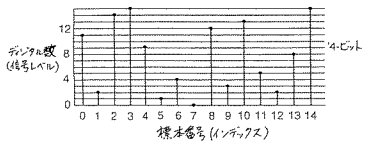
【図20】回転対象パターンを使用する実施形態に関する詳細を示す。

【図21】画素よりも“バンプ”の符号化を示す。

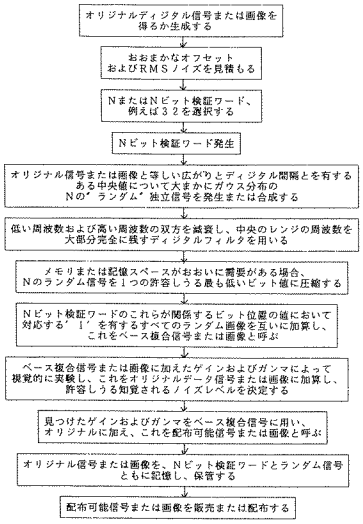
【図22】セキュリティカードの態様を詳細に示す。

【図23】セキュリティカードの態様を詳細に示す。
【図24】セキュリティカードの態様を詳細に示す。
【図25】セキュリティカードの態様を詳細に示す。
【図26】セキュリティカードの態様を詳細に示す。
【図27】固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク方法を説明する図である。
【図27A】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図27B】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図28】写真識別文書またはセキュリティカードの図である。
【図29】サブリミナルディジタルグラティキュールを実現することができる２つの実施形態を示す。
【図29A】図２９の実施形態における変形例を示す。
【図30】サブリミナルディジタルグラティキュールを実現することができる２つの実施形態を示す。
【図31】Ａ及びＢは、２つの傾斜軸に沿った空間周波数の位相を示す。
【図32】Ａ～Ｃは、第１、第２および第３同心リングに沿った空間周波数の位相を示す。
【図33】Ａ～Ｅは、傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34】Ａ～Ｅは、同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図35】Ａ～Ｃは、傾斜軸を使用するサブリミナルグラティキュールに対する他のステップを示す。
【図36】Ａ～Ｄは、２Ｄ　ＦＦＴを必要としない他の登録プロセスを示す。
【図37】サブリミナルグラティキュールに対する登録プロセスを要約するフローチャートである。
【図38】好例の無線電話システムの主な部品を示すブロック図である。
【図39】図３８のシステムの電話において使用することができる好例のステガノグラフィ的エンコーダのブロック図である
【図40】図１のセルサイトにおいて使用することができる好例のステガノグラフィ的デコーダのブロック図である
【図41】ＡおよびＢは、符号化の一形態において使用する好例のビットセルを示す。

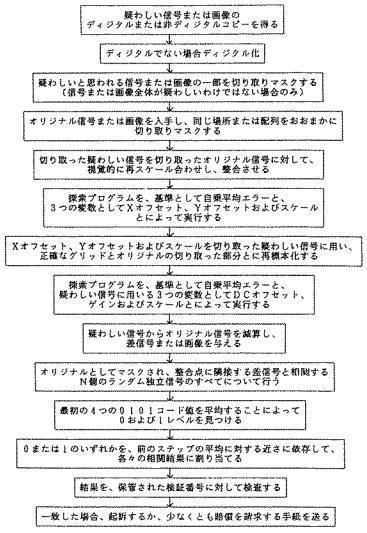
【図1】


12
8
4
0
ディジタル数
(信号レベル)
4-ビット
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
標本番号(インデックス)

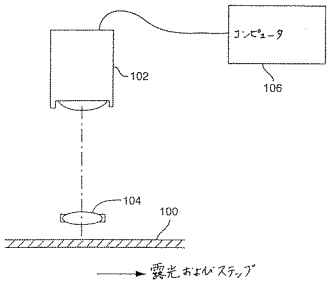
【図2】


オリジナルディジタル信号または画像を得るか生成する
おおまかなオフセットおよびＲＭＳノイズを見積もる
ＮまたはＮビット検証ワード、例えば３２を選択する
Ｎビット検証ワード発生
オリジナル信号または画像と等しい広がりとディジタル間隔とを有するある中央値について大まかにガウス分布のＮの"ランダム"独立信号を発生または合成する
低い周波数および高い周波数の双方を減衰し、中央のレンジの周波数を大部分完全に残すディジタルフィルタを用いる
メモリまたは記憶スペースがおおいに需要がある場合、Ｎのランダム信号を１つの許容しうる最も低いビット値に圧縮する
Ｎビット検証ワードのこれらが関係するビット位置の値において対応する"１"を有するすべてのランダム画像を互いに加算し、これをベース複合信号または画像と呼ぶ
ベース複合信号または画像に加えたゲインおよびガンマによって視覚的に実験し、これをオリジナルデータ信号または画像に加算し、許容しうる知覚されるノイズレベルを決定する
見つけたゲインおよびガンマをベース複合信号に用い、オリジナルに加え、これを配布可能信号または画像と呼ぶ
オリジナル信号または画像を、Ｎビット検証ワードとランダム信号ともに記憶し、保管する
配布可能信号または画像を販売または配布する

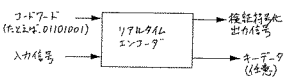
【図3】


疑わしい信号または画像のディジタルまたは非ディジタルコピーを得る
ディジタルでない場合ディジタル化
疑わしいと思われる信号または画像の一部を切り取りマスクする（信号または画像全体が疑わしいわけではない場合のみ）
オリジナル信号または画像を入手し、同じ場所または配列をおおまかに切り取りマスクする
切り取った疑わしい信号を切り取ったオリジナル信号に対して、視覚的に再スケール合わせし、整合させる
探索プログラムを、基準として自乗平均エラーと、３つの変数としてＸオフセット、Ｙオフセットおよびスケールとによって実行する
Ｘオフセット、Ｙオフセットおよびスケールを切り取った疑わしい信号に用い、正確なグリッドとオリジナルの切り取った部分とに再標本化する
探索プログラムを、基準として自乗平均エラーと、疑わしい信号に用いる３つの変数としてＤＣオフセット、ゲインおよびスケールとによって実行する
疑わしい信号からオリジナル信号を減算し、残信号または画像を与える
オリジナルとしてマスクされ、整合点に隣接する差信号と相関するＮ個のランダム独立信号のすべてについて行う
最初の４つの０１０１コード値を平均することによって０およびｌレベルを見つける
０またはｌのいずれかを、前のステップの平均に対する近さに依存して、各々の相関結果に割り当てる
結果を、保管された検証番号に対して検査する
一致した場合、起訴するか、少なくとも賠償を請求する手紙を送る

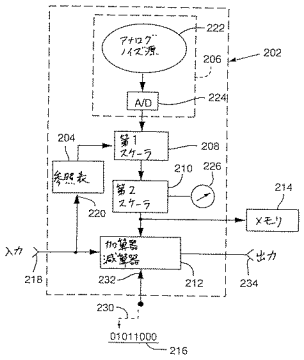
【図4】


コンピュータ
102
106
104
100
露光およびステップ

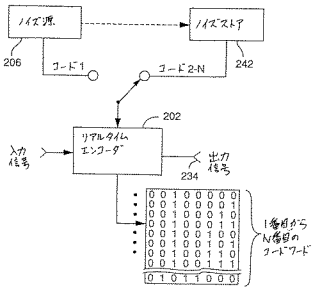
【図5】


コードワード
(たとえば、01101001)
入力信号
リアルタイム
エンコーダ
検証符号化
出力信号
キーデータ
(任意)

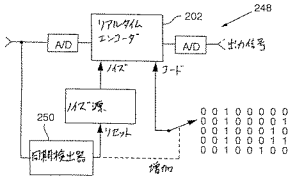
【図6】


アナログ
ノイズ源
222
206
202
A/D
224
204
第1
スケーラ
208
参照表
210
226
第2
スケーラ
214
メモリ
220
入力
加算器
減算器
出力
218
232
212
234
230
01011000
216

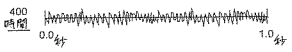
【図7】


ノイズ源
ノイズストア
206
コード1
コード2-N
242
202
リアルタイム
エンコーダ
入力
信号
出力
信号
234
1番目から
N番目の
コードワード

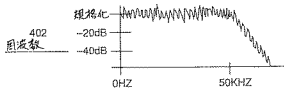
【図8】


リアルタイム
エンコーダ
202
248
A/D
A/D
出力信号
ノイズ
コード
ノイズ源
250
同期検出器
リセット
埋め

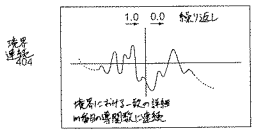
【図9A】



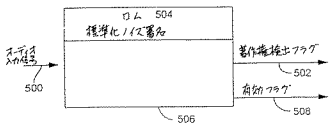
【図9B】



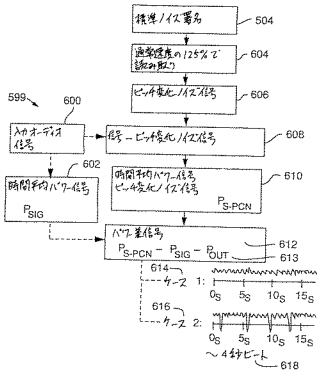
【図9C】



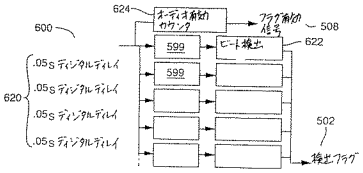
【図10】



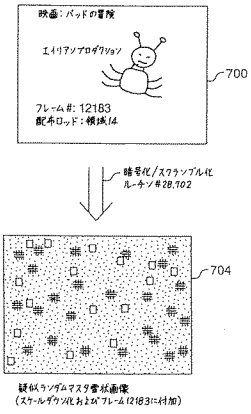
【図11】



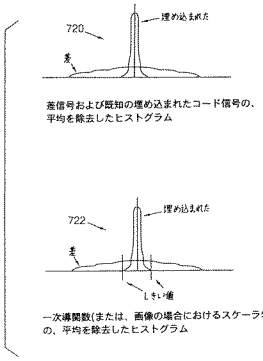
【図12】



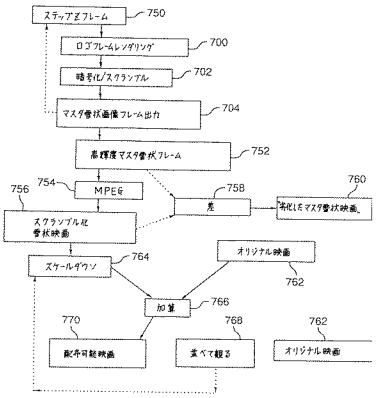
【図13】



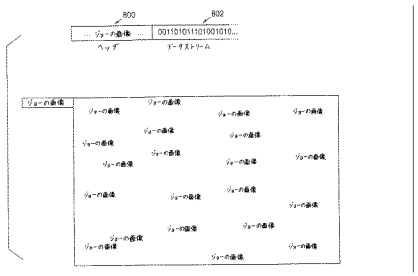
【図14】



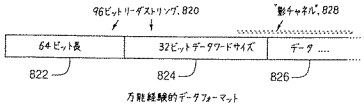
【図15】



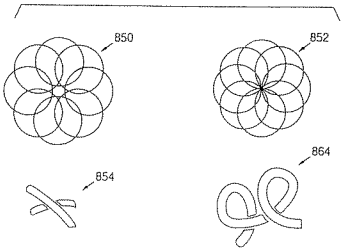
【図16】



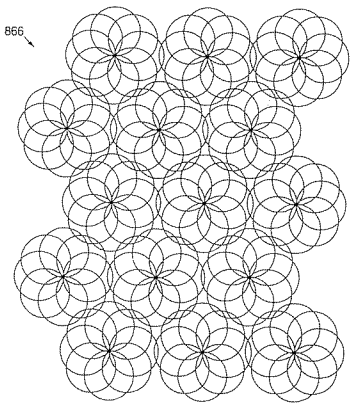
【図17】



【図18】

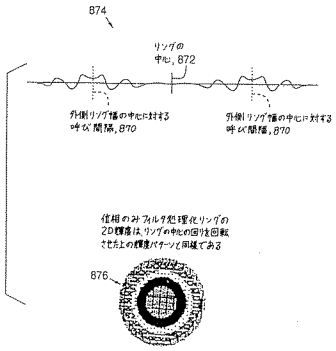


【図19】

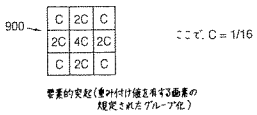


オリジナル画像を覆い、これと同一空間のモザイク化ノットパターンの探索; すべての要素ノットパターンは、署名のような同じ情報を輸送することができ、または、各々が、ステガノグラフィ的意味における新たなメッセージを輸送することができる。

【図20】

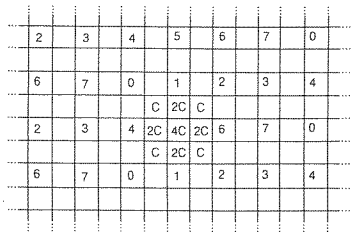


【図21A】



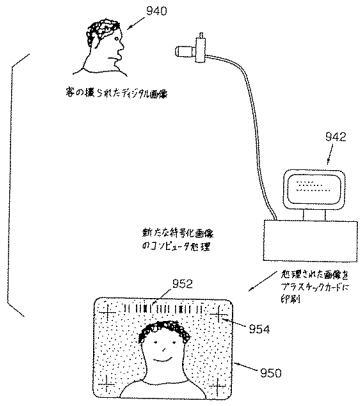
要素的変起(重み付け値を有する画素の
規定されたグループ化)

【図21B】

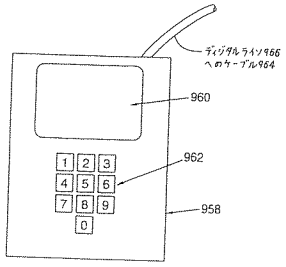


多くの要素的バンプを画像中の場所にどのように割り当て、これらの場所をNビットワードにおける対応するビットプレーンにどのように関連づけるかの例であり、ここで、0-7のインデックスを有するN=8とする。ビットプレーン"5"に関係する場所は、示したバンププロファイルの上敷きを有する。

【図22】



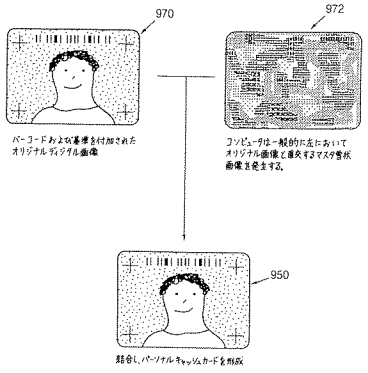
【図23】



基本的な光学スキャナ、メモリバッファ、通信装置およびマイクロプロセッサを含む。

客は単に、プラスチックカードを窓に置き、パーソナル識別番号(付加したセキュリティのために置く)か、そうでないかを予め任意に決めることができる。商取り引きは、数秒以内に承認または否認される。

【図24】

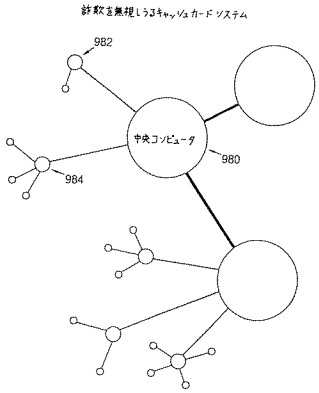


【図25】

代表的な商取り引きステップ

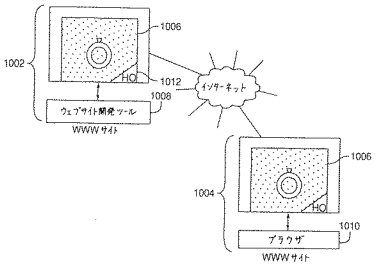
1. 読み取り装置が、メモリに格納された画像を走査し、人物のIDを抽出
2. 任意; PIN番号におけるユーザキー
   3. 読み取り装置が、中央口座データネットワークを呼び、ハンドシェーク
   4. 読み取り装置が、ID、{PIN}、商人情報、および必要な商取り引き量を中央ネットワークに送る
   5. 中央ネットワークが、ID、PIN、商人情報、および口座バランスを識別
   6. OKならば、中央ネットワークが16の異なったランダム番号の24の組を発生し、ここで、ランダム番号を、64K直交空間パターンの組に対するインデックスとする
   7. 中央ネットワークが、第1のOKと、ランダム番号の組とを送信する
8. 読み取り装置が、24の組を選む
   8A. 読み取り装置が、直交パターンの組を合計する
   8B. 読み取り装置が、結果として生じるパターンと、カード走査とのドット積を行い、結果を格納
   9. 読み取り装置が、24のドット積を中央ネットワークに送信
      10. 中央ネットワークが、結果をマスタに対して検査
      11. 中央ネットワークが、最終的な承認または否認を送る
      12. 中央ネットワークが、承認口座の借り方に記入し、カードロ座の貸し方に記入する

【図26】

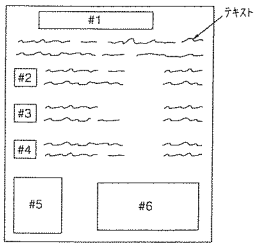


キャッシュカードシステムの基礎は、物理的カードシステム950を形成する局および売り点984の双方が、すべて同じネットワークに連続して接続される、24時間情報ネットワークである。

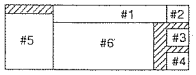
【図27】



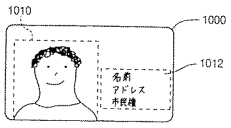
【図27A】



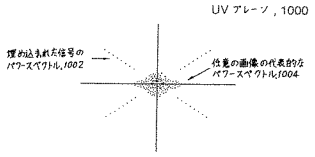
【図27B】



【図28】

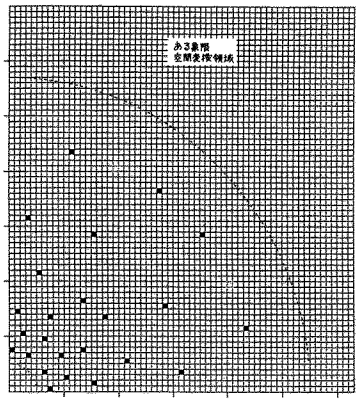


【図29】

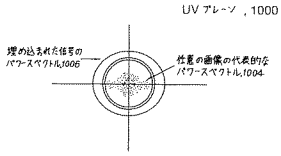


空間領域におけるクロスハッチングパターンのような波を生じる、45度軸に沿った非調和空間周波数

【図29A】

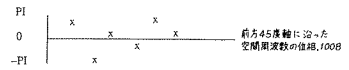


【図30】

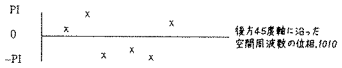


空間領域における疑似ランダム様パターンを生じる、位相が各々の円に沿って疑似ランダムに跳ねる、UVプレーンにおける非調和同心リング

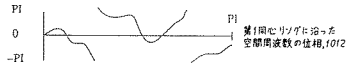
【図31A】



【図31B】

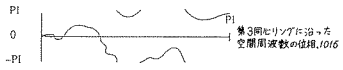


【図32A】

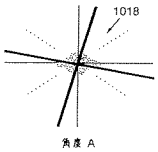


【図32B】

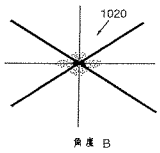
【図32C】



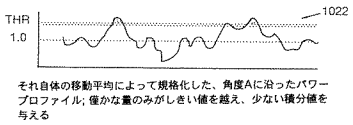
【図33A】



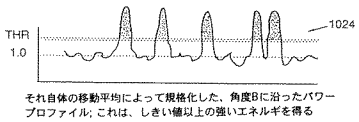
【図33B】



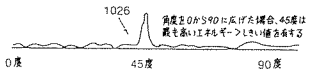
【図33C】



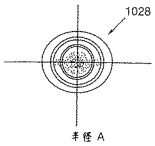
【図33D】



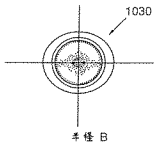
【図33E】



【図34A】

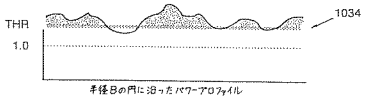


【図34B】

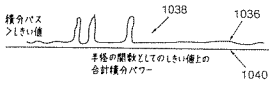


【図34C】

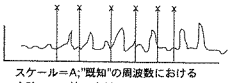
【図34D】



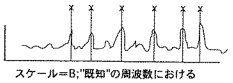
【図34E】



【図35A】

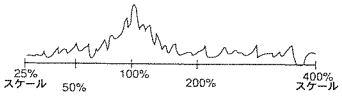


【図35B】



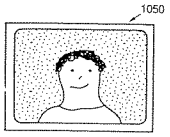
スケール＝B;"既知"の周波数における
合計パワー値, 1044

【図35C】



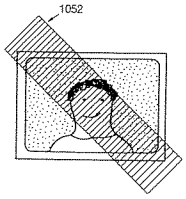
整合フィルタを基礎とする"スケール化カーネル";
ピークは、サブリミナル格子のスケールが見つかる場所, 1046

【図36A】



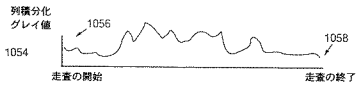
サブリミナルグラティキュール
が配置されているかもしれない
任意のオリジナル画像。

【図36B】

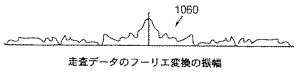


"列走査"を、画像の中心を通って
所定の角度に沿って用いる。

【図36C】



【図36D】

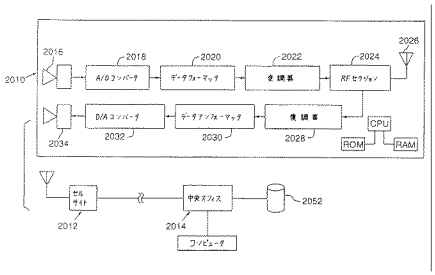


【図37】

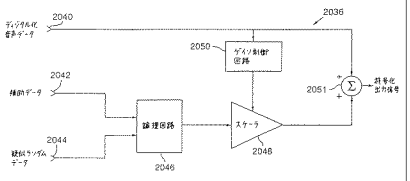
プロセスステップ

1. 写真における走査
2. 2D FFT
3. 2Dパワースペクトル発生、例えば、3×3ブラーリングカーネル
4. 0度から90度まで角度ステップ(1/2度)
5. 分子としてパワー値、分母として動き平均化パワー値による、規格化ベクトル発生
6. この角度に対する1つの積分値を与える、あるしきい値として値を積分
7. 角度におけるステップ終了
8. ループ4おける角度から、1つまたは2つまたは3つの"ピーク"を見つける
9. スケールを、25%から400%までステップ-0.01でステップ
10. 標準の"N"のスケール化周波数に対応する規格化パワー値を加算
11. ループにおける最高値のトラックを保持
12. ループ9および8を終了、最高値を決定
13. ここで見つけた回転およびスケール
14. 情例的な整合フィルタ処理を行い、正確な空間オフセットを見つける
15. 何らかの"細かい調整"を行い、回転、スケール、オフセットを正確に決定

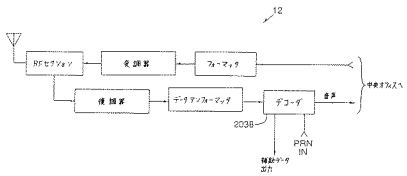
【図38】



【図39】



【図40】



【図41A】

【図41B】

【手続補正書】
【提出日】平成16年12月21日(2004.12.21)
【手続補正1】
【補正対象書類名】明細書
【補正対象項目名】０４９９
【補正方法】変更
【補正の内容】
【0499】
【図1】２つの軸において分離された１次元ディジタル信号の簡単かつ古典的な線図である。
【図2】“微細の”認証信号を他の信号上に埋め込む処理の、ステップの詳細な記述による全体的な概観である。
【図3】オリジナルの疑わしいコピーをどのように検証するかについての漸次の説明である。
【図4】本発明の他の実施例による検証情報によってフィルムを前露光する装置の線図である。
【図5】本発明の“ブラックボックス”実施例の図表である。
【図6】図５の実施例のブロック図である。
【図7】異なったコードワードを有するが同じノイズデータを有する入力データの連続する組を符号化するのに適合した図６の実施例の変形例を示す。
【図8】特有のコード番号を有するビデオテープ製造の各々のフレームを符号化するのに適合した図６の実施例の変形例を示す。
【図9A】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図9B】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図9C】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図10】標準ノイズコードの検出において使用される集積回路を示す。
【図11】図１０の実施例において使用することができる標準ノイズコードを検出する処理の流れを示す。
【図12】本発明の他の実施例による複数の検出器を使用する実施例である。
【図13】疑似ランダムノイズフレームを画像から発生する実施形態を示す。
【図14】信号の統計を復号化の援助においてどのように使用できるかを示す。
【図15】どのように署名信号を使用し、予測される歪み（例えば、ＭＰＥＧ）の視点におけるその堅牢さを増すかを示す。
【図16】ファイルについての情報をヘッダおよびファイル自体において詳述する実施形態を示す。
【図17】ファイルについての情報をヘッダおよびファイル自体において詳述する実施形態を示す。
【図18】回転対象パターンを使用する実施形態に関する詳細を示す。
【図19】回転対象パターンを使用する実施形態に関する詳細を示す。
【図20】回転対象パターンを使用する実施形態に関する詳細を示す。
【図21A】画素よりも“バンプ”の符号化を示す。
【図21B】画素よりも“バンプ”の符号化を示す。
【図22】セキュリティカードの態様を詳細に示す。
【図23】セキュリティカードの態様を詳細に示す。
【図24】セキュリティカードの態様を詳細に示す。
【図25】セキュリティカードの態様を詳細に示す。
【図26】セキュリティカードの態様を詳細に示す。

【図27】固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク方法を説明する図である。
【図27A】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図27B】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図28】写真識別文書またはセキュリティカードの図である。
【図29】サブリミナルディジタルグラティキュールを実現することができる２つの実施形態を示す。
【図29A】図２９の実施形態における変形例を示す。
【図30】サブリミナルディジタルグラティキュールを実現することができる２つの実施形態を示す。
【図31A】２つの傾斜軸に沿った空間周波数の位相を示す。
【図31B】２つの傾斜軸に沿った空間周波数の位相を示す。
【図32A】第１、第２および第３同心リングに沿った空間周波数の位相を示す。
【図32B】第１、第２および第３同心リングに沿った空間周波数の位相を示す。
【図32C】第１、第２および第３同心リングに沿った空間周波数の位相を示す。
【図33A】傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図33B】傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図33C】傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図33D】傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図33E】傾斜軸を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34A】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34B】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34C】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34D】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図34E】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。
【図35A】傾斜軸を使用するサブリミナルグラティキュールに対する他のステップを示す。
【図35B】傾斜軸を使用するサブリミナルグラティキュールに対する他のステップを示す。
【図35C】傾斜軸を使用するサブリミナルグラティキュールに対する他のステップを示す。
【図36A】２Ｄ　ＦＦＴを必要としない他の登録プロセスを示す。
【図36B】２Ｄ　ＦＦＴを必要としない他の登録プロセスを示す。
【図36C】２Ｄ　ＦＦＴを必要としない他の登録プロセスを示す。
【図36D】２Ｄ　ＦＦＴを必要としない他の登録プロセスを示す。
【図37】サブリミナルグラティキュールに対する登録プロセスを要約するフローチャートである。
【図38】好例の無線電話システムの主な部品を示すブロック図である。

【図39】図３８のシステムの電話において使用することができる好例のステガノグラフィ的エンコーダのブロック図である。
【図40】図１のセルサイトにおいて使用することができる好例のステガノグラフィ的デコーダのブロック図である。
【図41A】符号化の一形態において使用する好例のビットセルを示す。
【図41B】符号化の一形態において使用する好例のビットセルを示す。

(31)優先権主張番号　08/635,531
(32)優先日　　平成8年4月25日(1996.4.25)
(33)優先権主張国　　米国(US)

（特許庁注：以下のものは登録商標）
１．フロッピー
２．ＪＡＶＡ
３．ペンティアム